(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
25. Januar 2001 (25.01.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/06341 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP00/06824

(22) Internationales Anmeldedatum:
17. Juli 2000 (17.07.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 32 703.3 15. Juli 1999 (15.07.1999) DE

(71) Anmelder und
(72) Erfinder: WITTKÖTTER, Erland [DE/CH]; Schönhaldestrasse 21, CH-8272 Ermatingen (CH).

(74) Anwälte: BEHRMANN, Niels usw.; Hiebsch Peege Behrmann, Heinrich-Weber-Platz 1, 78224 Singen (DE).

(81) Bestimmungsstaaten *(national)*: IN, JP, US.

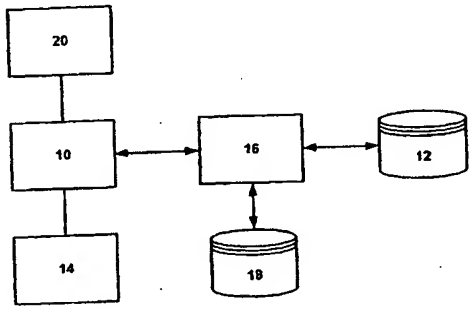
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

[Fortsetzung auf der nächsten Seite]

(54) Title: DATA PROCESSING DEVICE

(54) Bezeichnung: DATENVERARBEITUNGSVORRICHTUNG



(57) Abstract: The invention relates to a data processing device comprising a local file receiving system which is used to receive local files and which is associated with a local computer unit and used for the purpose of retrieval and storage, in addition to two-way transmission of volume files by the computer unit, and a user identification unit which is associated with the local computer unit and which is configured in such a way that it can react to positive ID only in order to enable access by said computer unit to volume files which are authorized for a user. The volume file is stored in the local file receiving system in an encrypted form which cannot be used for a user. A key administration system which is associated with a volume file transmission path between the local computer unit and local file receiving system is configured as part of and as a functionality of the local computer unit for the generation and allocation of a user-specific and volume-file-specific key data file for each volume file. The key management system is connected to a key data base which is part of the system for receiving local files and logically separated therefrom. The key management system links a key file which is stored in the key data base to a volume file stored in the local file receiving system in order to generate an electronic document so that a volume file can be produced for the local file receiving system. The key data base is provided locally in the data processing unit but is structurally or physically separated from the driver unit or mass storage unit which is associated with the local file receiving system.

(57) Zusammenfassung: Die Erfindung betrifft eine Datenverarbeitungsvorrichtung mit einem einer lokalen Rechnereinheit zugeordneten lokalen Dateiablagesystem zum Abrufen und zur Speicherung sowie zur bidirektionalen Datenübertragung von Volumendateien mittels der Rechnereinheit und einer der lokalen Rechnereinheit zugeordneten Nutzer-Identifikationseinheit, die zum Ermöglichen eines Zugriffs durch die Rechnereinheit auf

[Fortsetzung auf der nächsten Seite]

WO 01/06341 A1

— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

für einen Nutzer autorisierte Volumendateien nur als Reaktion auf dessen positive Identifikation ausgebildet ist, wobei die Volumendatei in dem lokalen Dateiablagesystem in einer für einen Nutzer nicht brauchbaren, verschlüsselten Form gespeichert ist, wobei eine einem Datenübertragungspfad von Volumendateien zwischen der lokalen Rechnereinheit und dem lokalen Dateiablagesystem zugeordnete Schlüsselverwaltungseinheit als Teil und Funktionalität der lokalen Rechnereinheit, die zum Erzeugen und Zuweisen einer nutzerspezifischen und volumendateispezifischen Schlüsseldatei für jede Volumendatei ausgebildet ist, die Schlüsselverwaltungseinheit mit einer als Teil des lokalen Dateiablagesystems, von diesem logisch getrennt vorgesehenen Schlüsseldatenbank verbunden ist und zum Verknüpfen einer in der Schlüsseldatenbank gespeicherten Schlüsseldatei mit einer im lokalen Dateiablagesystem gespeicherten Volumendatei zum Erzeugen eines für einen Nutzer brauchbaren eleketronischen Dokuments sowie zum Verknüpfen einer erzeugten Schlüsseldatei mit einem zu speichernden elektronischen Dokument zum Erzeugen einer Volumendatei für das lokale Dateiablagesystem ausgebildet ist, wobei die Schlüsseldatenbank lokal in der Datenverarbeitungsvorrichtung, jedoch strukturell oder physisch getrennt von einer dem lokalen Dateiablagesystem zugeordneten Laufwerks- oder Massenspeichereinheit vorgesehen ist.

BESCHREIBUNG

Datenverarbeitungsvorrichtung

Die vorliegende Erfindung betrifft eine Datenverarbeitungsvorrichtung nach dem Oberbegriff des Patentanspruchs 1.

Vor dem Hintergrund zunehmend strengerer Erfordernisse an die Datensicherheit, den Schutz vor unerlaubtem Datenzugriff durch Dritte sowie des unautorisierten Kopierens ganzer Daten- und Dateistrukturen bzw. des unautorisierten Zugriffs und Einblicks auf/in diese stellt sich das generelle Problem des Zugriffsschutzes auf Nutzerdateien nicht nur für Großrechnersysteme oder für unternehmensweite Netzwerke; oftmals sind auch bereits Einzelplatzsysteme oder kleine, lokale Rechnerverbünde bedroht.

Zugangsregelung und Zugriffsschutz hat daher Eingang in praktisch alle Rechnerbetriebssysteme und Anwenderprogramme gefunden, von einem passwortgeschützten Rechnerstart (der nämlich überhaupt erst das Hochfahren eines Betriebssystems ermöglicht, wenn ein korrektes Passwort eingegeben wurde), bis hin zu individueller Zugriffssicherung etwa von mit einem Anwendungsprogramm, z. B. einer Textverarbeitung, erstellten elektronischen Dokumenten (als "elektronisches Dokument" sollen im folgenden beliebige, für einen Nutzer brauchbare, d. h. sinnvoll mit dem beabsichtigten Inhalt bzw. Kommunikationszweck belegte, les-, erkenn- und ausgebbare Nutzdateien, eingeschlossen ausführbare Programme, verstanden werden, im praktischen Gebrauch sind dies beispielsweise Texte, Bilder, Ton- und/oder Bildfolgen, 3-D-Animationen, interaktive Eingabemasken usw.).

Gerade im Anwendungsfeld eines lokalen Arbeitsplatzes oder Rechnerverbundes bieten aber passwortgeschützte Zugriffs- oder Startroutinen üblicherweise einen nur ungenügenden Schutz: Selbst wenn, etwa durch Passwortschutz eines Arbeitsplatzcomputers als über das betreffende Betriebssystem angebotenem Zugriffsschutz der Rechner, durch einen unautorisierten Benutzer nicht gestartet werden kann, so besteht die Gefahr, dass entweder über Umwege auf den diesem Arbeitsplatzrechner zugeordneten Massenspeicher zugegriffen wird, oder aber einfach, etwa im Wege einer Backup-Routine, der komplette Inhalt eines solchen Massenspeichers, etwa einer Festplatte, ausgelesen und dann zu einem späteren Zeitpunkt mit einem anderen System widerrechtlich analysiert und gelesen wird.

Auch ein individueller Dokumenten-Passwortschutz verspricht gegen derartige, unautorisierte Backups einen nur ungenügenden Schutz, denn selbst auf einer Festplatte passwort-verschlüsselte Nutzdateien können oftmals mit geringem Aufwand, unter Ausnutzung der inhä-

renten, inneren Redundanz von Bildern oder Sprache, in ihre ursprüngliche, offene Fassung zurückversetzt werden. Ein derartiger, Dokument-individueller Passwortschutz, der üblicherweise auch als Benutzer-Level-Kryptografie verstanden wird, ist, bedingt durch seine strikte Dokumentabhängigkeit, empfindlich gegen Bedienfehler und umständlich: Es besteht die Gefahr, dass ein Benutzer das Verschlüsseln einzelner Dateien vergißt oder aber eine ursprünglich unverschlüsselte Textdatei nach dem verschlüsselten Abspeichern nicht löscht. Auch ist die Benutzung wenig komfortabel, da üblicherweise während einer Benutzersitzung (Session) ein zugehöriges Passwort mehrfach einzugeben ist. Insbesondere im Zusammenhang mit File-Servern in einer vernetzten Umgebung ist es zudem praktisch unvermeidbar, dass zumindest zu gewissen Zeitpunkten sich eine klare, unverschlüsselte Nutzerdatei auf einem Speichermedium befindet und so etwa über ein Netzwerk offener Zugriff möglich ist.

Als weiterer Nachteil einer solchen, aus dem Stand der Technik bekannten Lösung, wie sie etwa im Zusammenhang mit gängigen Textverarbeitungssystemen bekannt ist, besteht darin, daß ein jeweiliger Benutzer sich ein zugehöriges Passwort merken muss, die Gefahr durch Dokumentverlust bei Verlieren des Passwortes also groß ist, und darüber hinaus eine Entschlüsselung jeweils nur programm- bzw. anwendungsspezifisch ist, also insbesondere ein Zugriff auf eine dergestalt verschlüsselte Datei mit anderen Anwendungsprogrammen und deren Weiterverwendung stark erschwert, wenn nicht gar unmöglich ist.

Wie zudem bereits erwähnt, besteht der prinzipbedingte Nachteil einer klassischen Verschlüsselung mit Hilfe von bekannten kryptografischen Verfahren (symmetrische oder asymmetrische Verschlüsselung wie DES, IDEA, RSA, El-Gamal) in der Abhängigkeit von der Geheimhaltung eines relativ kurzen Schlüssels, üblicherweise 56 bzw. 128 Bit. Wenn ein solcher Schlüssel aufgrund der erwähnten inneren Redunanz der Sprache oder des Standards, in der das betreffende elektronische Dokument verfasst worden ist, aus einem begrenzten Datenkontext berechnet werden kann, dann ist somit der gesamte Inhalt, bei dem dieser Schlüssel verwendet worden ist, lesbar.

Ein weitere Problem bilden sog. offene Systeme, die durch Multiuser-Betriebssysteme verwaltet werden und Zugriffe auf Netzwerk-Massenspeicher ermöglichen. Ein solcher Zugriff wird üblicherweise über das Betriebssystem nur unzureichend verwaltet, und insbesondere kann darüber hinaus im Normalfall nicht nachvollzogen werden, wer, wann und von wo Daten geschrieben oder gelesen hat. Dagegen ist offensichtlich, dass insbesondere in einem vertraulichen Kontext derartige Informationen, etwa im Fall späterer Beweisführungen, zum verbesserten Quellenschutz notwendig sein können.

Aufgabe der vorliegenden Erfindung ist es daher, eine gattungsgemäße Datenverarbeitungsvorrichtung im Hinblick auf die Datensicherheit von lokal gespeicherten Nutz- bzw. Volumendaten zu verbessern, und insbesondere die Gefahr durch unautorisierten Datenzugriff durch vollständiges Kopieren eines Massenspeicherinhalts, etwa durch Backup, zu vermindern. Insbesondere sind zudem auch die Sicherheitsnachteile bekannter Kryptografieverfahren gegen Entschlüsselung zu überwinden und die Verschlüsselungssicherheit zu erhöhen.

Die Aufgabe wird durch die Vorrichtung mit den Merkmalen des Patentanspruchs 1 und 10 sowie die Verfahren mit den Schritten der Patentansprüche 7 und 8 gelöst; bevorzugte Weiterbildungen der Erfindung ergeben sich aus den rückbezogenen, abhängigen Ansprüchen.

In erfindungsgemäß vorteilhafter Weise findet eine Abkehr von dem gerade im Einzelplatz- bzw. lokalen Netzwerkbereich üblichen rollenspezifischen (d.h. auf Benutzer, z.B. Administrator, bezogenen) Passwortprinzip statt, und ein Schutz der sicherheitsbedürftigen Nutzerdateien -- im weiteren und im Rahmen der Erfindung auch als Volumendateien bezeichnet -- erfolgt durch die erfindungsgemäß zusätzlich vorgesehene Schlüsselverwaltungseinheit im Zusammenwirken mit der Schlüsselspeichereinheit ("Schlüsseldatei").

Genauer gesagt besteht ein wesentliches Merkmal der vorliegenden Erfindung darin, jegliche (bzw. eine ausgewählte und/oder vom Betriebssystem bestimmte), zur -- zugriffsgeschützten -- Speicherung sowie zum späteren Wieder-Aufrufen vorgesehene Datei vor ihrer Ablage im lokalen Dateiablagesystem, welche besonders bevorzugt ein üblicher Massenspeicher, etwa eine Festplatte, ein optisches Laufwerk usw. sein kann, zu verschlüsseln, und zwar mittels eines sowohl datei- als auch benutzerspezifischen Schlüssels. Damit ist gemeint, dass jede im Rahmen der vorliegenden Erfindung zu sichernde Volumendatei, bevorzugt die Gesamtheit der auf dem Dateiablagesystem zu speichernden Dateien, mit einem individuellen Schlüssel versehen wird, der getrennt (also nicht in einer dem Dateiablagesystem unmittelbar zugeordneten Weise) gespeichert wird, und eine Volumendatei nur zusammen mit dem zugehörigen, individualisierten Schlüssel offen und benutzbar wird. Auch bedeutet die nutzerspezifische Eigenschaft eines Schlüssels, dass für verschiedene Nutzer der erfindungsgemäßen Datenverarbeitungsvorrichtung eine jeweilige Zugehörigkeits- und Autorisierungsprüfung stattfindet, also ein Nutzer (im Rahmen der Erfindung ist als "Nutzer" insoweit auch eine Benutzer*gruppe* zu verstehen) kann im Rahmen der vorliegenden Erfindung nur auf die für ihn vorgesehenen bzw. autorisierten Volumendateien zugreifen, und dies wird -- abweichend vom Stand der Technik -- insbesondere auch über die individualisierte Schlüsseldatei bzw. Schlüsseldatensatz einer Datenbank erreicht.

In der praktischen Realisierung der Erfindung muss also vor jeder Arbeitssitzung mit Zugriff auf -- als solche nicht benutzbare -- Volumendateien eine mindestens einmalige Identifikation und Autorisierung eines jeweiligen Nutzers stattfinden, und erst durch Verknüpfung mit einer getrennt gespeicherten bzw. erzeugten Schlüsseldatei kann eine in dem Dateiablagesystem bevorzugt dauerhaft gespeicherte Volumendatei gesichert bzw. in nutzbarer Form verwendet werden.

Nicht nur wird damit das Hauptproblem bestehender, passwortgeschützter Datenverarbeitungssysteme aus dem Stand der Technik gelöst (auch ein vollständiges Kopieren einer Festplatte mit dem Dateiablagesystem ermöglicht keinen Zugriff auf die benutzbaren Nutzerdaten), durch Zwischenschaltung der erfindungsgemäßen Schlüsselverwaltungseinheit in den bidirektionalen Speicher- und Aufrufpfad zwischen Rechnereinheit und lokalem Dateisystem werden diese Sicherungsvorgänge für einen autorisierten Benutzer -- nach einmaliger, erfolgreicher Identifikation -- unsichtbar und unbemerkt, bieten also beispielsweise den Vorteil, im Verlauf einer Arbeitssitzung am Datenverarbeitungssystem (session) nicht bei jedem neuen Öffnen einer Textdatei ein zugehöriges Passwort eingeben zu müssen.

Der weitere Vorteil einer erfindungsgemäß benutzer- und dateispezifischen Verschlüsselung besteht zudem darin, dass im Fall des Bekanntwerdens eines individuellen Schlüssels der notwendige Aufwand für eine Schlüsseländerung oder Zugriffsänderung relativ gering bleibt.

Weiterbildungsgemäß ist es im Rahmen der Erfindung vorgesehen, zum Zugriff auf den Schlüssel eine weitere, in Form einer verschlüsselten Zwischendatei (Zwischenschicht) realisierte, nicht auf einer gemeinsamen Back-Up-Einheit gespeicherte Sicherungsebene vorzusehen, die insbesondere die Sicherheit des Zugriffs auf den Schlüssel weiter erhöht. Durch eine solche, selbst verschlüsselte, physisch entfernte Zwischenlage ist damit sichergestellt, dass die eigentliche Schlüsseldatei nicht direkt zugänglich ist.

Als Ergebnis der vorliegenden Erfindung ergibt sich zudem, dass prinzipiell das Lesen des verschlüsselten Dateiablagesystems, etwa zum Zweck des Backups, als solches erlaubt und allgemein zugänglich ist und insbesondere von einer Autorisierung unabhängig gemacht wird (da ja auch das Ergebnis eines solchen Backups verschlüsselt bleibt). Entsprechend werden derartige Sicherungsvorgänge, wie der Backup-Prozess, von etwa einem besonderen, sicheren Zugriffstatus (üblicherweise Supervisor oder Systemadministrator) unabhängig, da das eigentliche Leserecht bzw. die Fähigkeit, auf das elektronische Dokument im Klartext (d.h. offen und unverschlüsselt) zuzugreifen, unabhängig von der Backup-Funktion und damit von einem Supervisor od.dgl. vergeben werden kann.

Gemäß einer bevorzugten Weiterbildung der Erfindung, für die auch unabhängiger Schutz beansprucht wird, werden zudem semantische, d. h. inhalts- und/oder sinnentstellende Verschlüsselungsverfahren, herangezogen, wobei hier der zu schützende Inhalt einer Volumendatei eine entsprechend unbrauchbare Fassung erhält und erst durch eine zugehörige, dateisowie nutzerindividualisierte Schlüsseldatei, die dann beispielsweise einen Reihenfolgeindex für eine korrekte Anordnung vertauschter Einzelbegriffe oder Sätze eines Textes enthält, in der Kombination einen so verschlüsselten Text verständlich macht.

Eine derartige semantische Verschlüsselung bietet gegenüber klassischen Kryptografieverfahren, insbesondere im vorliegenden Kontext der Verschlüsselung auf der Ebene des Filesystems, eine Vielzahl von Vorteilen: So ist zum einen die Verschlüsselungssicherheit, insbesondere bedingt durch die Möglichkeit, beliebige Informationskomponenten einzufügen bzw. auszutauschen, nahezu absolut, wobei insbesondere jegliche Kontext- bzw. Inhaltsabhängigkeit des Schlüssels vom verschlüsselten Text nicht mehr vorhanden ist. Auch läßt sich mit diesem Verschlüsselungsverfahren in besonders einfacher Weise einen Bezug zum jeweiligen Nutzer herstellen. Bei bestimmten ursprünglichen Datenmengen, etwa Texten, läßt sich zudem gemäß einer bevorzugten Weiterbildung der Erfindung eine Verschlüsselung dergestalt vornehmen, dass ein jeweiliger Inhalt zwar gegenüber dem ursprünglichen Inhalt entstellt und verändert wird, insoweit also aus Benutzersicht nutzlos wird, gleichwohl jedoch ein Sinn und/oder eine technische Lesbarkeit und Darstellbarkeit der verschlüsselten Datenmenge erhalten bleibt (mit der Wirkung, dass möglicherweise überhaupt nicht erkannt wird, dass eine Verschlüsselung vorliegt). Dies ist beispielsweise dann der Fall, wenn gewisse Worte und Begriffe eines Textes (die insoweit als Informationskomponenten im Sinne des Patentanspruches 8 verstanden werden) gegen semantisch und/oder grammatikalisch vergleichbare, inhaltlich jedoch anders aufzufassende Termini ersetzt werden.

Generell erfordert die vorliegende Erfindung eine Metasprache in Form einer linearen Verkettung von jeweils aus sich heraus sinngebenden Modulen (Informationskomponenten), die zum Zwecke des vorliegenden Verfahrens zerlegt und durch die Aktionen des Vertauschens, Entfernens, Hinzufügens und/oder Austauschens in die für den Nutzer unbrauchbare Form (Anordnung) gebracht wird.

Im Rahmen der vorliegenden Erfindung ist eine Vorrichtung zum Behandeln einer elektronisch gespeicherten ursprünglichen Datenmenge geschaffen, welche insbesondere zur Implementierung der vorstehend beschriebenen semantischen Verschlüsselung geeignet und vorgesehen ist.

In erfindungsgemäß vorteilhafter Weise wird durch eine solche Vorrichtung die Funktionalität einer Schlüsselerzeugungs- und Verwaltungseinheit realisiert, welche in der Lage ist, sowohl aus einem ursprünglichen, zu schützenden Dokument (nämlich der ursprünglichen Datenmenge bzw. Nutzdatei) die semantisch verschlüsselten Volumendaten nebst Schlüsseldaten zu erzeugen, als auch für eine Verwaltung und Weiterbehandlung der so erzeugten Datenmengen zu sorgen. So ist insbesondere die erfindungsgemäße Analyseeinheit vorgesehen, um im Rahmen der vorgegebenen Formatstruktur und/oder Grammatik des ursprünglichen Dokuments die Voraussetzung für eine nachfolgende inhalts- bzw. sinnbezogene Verschlüsselung zu schaffen, und die der Analyseeinheit nachgeschaltete Verschlüsselungseinheit nimmt dann die Kernoperationen der semantischen Verschlüsselung, nämlich das Vertauschen, Entfernen, Hinzufügen und Austauschen, auf die Informationskomponenten der ursprünglichen Datenmenge, unter Berücksichtigung der analysierten Formatstruktur und Grammatik, vor.

Dabei ist es besonders geeignet, etwa die Operationen des Vertauschens oder Austauschens so vorzunehmen, dass eine betreffende Informationskomponente mit bzw. durch inhaltlich, strukturell oder grammatikalisch äquivalente Informationskomponenten ersetzt wird, insoweit also das Resultat der Operation nach wie vor scheinbar sinnvoll bleibt. Die weiterbildungsgemäß vorgesehene Äquivalenzeinheit ermöglicht im Rahmen der vorliegenden Erfindung die Identifikation bzw. die Auswahl geeigneter äquivalenter Informationskomponenten für diese oder andere Operationen.

Gemäß einer weiteren, bevorzugten Weiterbildung der Erfindung findet zudem eine Operation durch die Verschlüsselungseinheit unter Berücksichtigung der Grammatik (der zugrunde liegenden natürlichen, maschinellen oder menschlichen Sprache), des Formats oder der Syntax des ursprünglichen Dokuments statt: Durch Wirkung der bevorzugt vorgesehenen semantischen Regeleinheit ist nämlich die erfindungsgemäß vorgesehene Verschlüsselungseinheit in der Lage, wiederum ein Verschlüsselungsergebnis zu erzeugen, welches eine der Ursprungsdatei entsprechende grammatikalische, formatmäßige und/oder syntaktische Struktur besitzt, so dass also nicht nur im Hinblick auf die jeweiligen einzelnen Informationskomponenten (z.B. Worte in einem Text) Äquivalenz gegeben ist, sondern auch im Hinblick auf die Strukturen und/oder formatmäßigen Anordnungen (also z.B. die Anordnung von Begriffen in einem Satz nach den Regeln der Grammatik) regelkonform ist und insoweit ohne inhaltliche Prüfung nicht erkennen läßt, dass eine den Verschlüsselungseffekt bewirkende Operation auf die Informationskomponenten stattgefunden hat. Als Äquivalenz im Rahmen der vorliegenden Erfindung wird insbesondere auch die sog. metaphorische Äquivalenz einbezogen. Als metaphorisch bzw. metaphorik im Rahmen der vorliegenden Erfindung sollen dabei jegliche Elemente einer Sprache verstanden werden, die in einem aus Verständnissicht sinnvollen

Zusammenhang zueinander stehen, also gewissermaßen einer gemeinsamen inhaltlichen, thematischen und/oder sinngebenen Gruppe von Sprachelementen (also z.B. Worten) angehören. Typische Beispiele für im Rahmen der vorliegenden Erfindung metaphorisch äquivalente Begriffe sind z.B. "Bahnhof" mit "Tankstelle" oder "Flughafen", als jeweilig unmittelbar thematisch dem Gebiet "Verkehr" zugehörig und insoweit metaphorisch austauschbar. Andere Beispiele sind Vornamen, Ortsbezeichnungen oder numerische Angaben (wie Datumsangaben, Währungsangaben usw.), die jeweils untereinander als metaphorisch äquivalent anzusehen sind.

Gemäß einer weiteren, bevorzugten Weiterbildung ist der Verschlüsselungseinheit eine Steuerungseinheit zugeordnet, welche den Verschlüsselungsbetrieb (d.h. die Anwendung und Wirkung der einzelnen verschlüsselnden Operationen) randomisiert: Durch Erzeugen und Berücksichtigen einer Zufallskomponente, z.B. einer in ansonsten bekannter Weise erzeugten Zufallszahl und deren Berücksichtigung bei dem Vornehmen einer davon abhängigen Anzahl von Verschlüsselungsoperationen, ist sichergestellt, dass ein Verschlüsseln desselben Ursprungsdokuments stets zu einem verschiedenen Ergebnis führt, also die Verschlüsselung selbst unter ansonsten identischen Bedingungen nie dasselbe Verschlüsselungsergebnis erzeugt. Auch mit dieser Maßnahme läßt sich die Sicherheit der vorliegenden Erfindung weiter erhöhen.

Generell hat es sich zudem als besonders bevorzugt bewährt, einem die Verschlüsselung anwendenden Benutzer die Möglichkeit zu geben, eine vorbestimmte Verschlüsselungstiefe (und damit eine Verschlüsselungssicherheit) vorzuwählen: Beim beschriebenen Erfindungsaspekt der semantischen Verschlüsselung korreliert die Frage der Verschlüsselungstiefe mit der Anzahl der durchgeführten, die Verschlüsselung bewirkenden Basisoperationen des Vertauschens, Entfernens, Hinzufügens oder Austauschens, und bestimmt insoweit auch das Volumen der erzeugten Schlüsseldatei. Durch Einstellen eines entsprechenden Parameters kann somit der Nutzer faktisch eine Sicherungsstufe der durchzuführenden Verschlüsselungsoperationen bestimmen, wobei jedoch, im Gegensatz zu bekannten, klassischen Verschlüsselungsverfahren, in jedem Fall das Ergebnis der semantischen Verschlüsselung ein scheinbar korrektes (d.h. scheinbar unverschlüsseltes) Ergebnis bringt, und die Frage, ob überhaupt eine Verschlüsselung stattgefunden hat, ohne inhaltliche (bzw. mit Vorwissen ausgestattete) Prüfung nicht möglich ist. Insoweit lässt sich also durch diesen durch die semantische Verschlüsselung erstmals erreichten Effekt der Unsicherheit sogar eine gewisse Schutzwirkung erreichen, ohne dass überhaupt eine einzige Verschlüsselungsoperation im vorbeschriebenen Sinne durchgeführt wird.

Als weitere, besonders bevorzugte Realisierungsform der vorliegenden Erfindung hat es sich zudem herausgestellt, mittels der weiterbildungsgemäß vorgesehenen Konvertierungseinheit die Volumendaten als Dokument auszugeben, während die Schlüsseldatei als lauffähige Scriptdaten einer geeigneten Struktur- oder Scriptsprache, z.B. XML, SGML, XSL, Visual Basic (Script), Javascript usw., erzeugt und ausgegeben werden kann, mit dem Vorteil, dass insbesondere im Zusammenhang mit Netz- oder Internet-basierten Anwendungen dann in besonders einfacher Weise ein Wiederherstellen der Ursprungsdaten erfolgen kann, im einfachsten Fall durch Ablaufen des das Wiederherstellen unmittelbar bewirkenden Scripts (welches über eine geeignete, das Interesse des Schutzsuchenden berücksichtigende Verbindung herangeführt worden ist), und welches zudem Ansatzpunkte für weitere Sicherheitsmechanismen, z.B. Datenintegrität oder Serverkontakt, bietet.

Im Ergebnis läßt sich so mit Hilfe der erfindungsgemäßen Infrastruktur eine hochgradig sichere und gleichwohl bedienungsfreundliche Schutzarchitektur schaffen, die nicht nur die Interessen des Schöpfers eines schutzwürdigen elektronischen Dokuments deutlich besser schützt als dies mit konventionellen Möglichkeiten gegeben ist, sondern die zudem auch potentiellen Nutzern des geschützten Inhaltes einen leichten, komfortablen Zugang und Umgang mit dem Dokument ermöglicht, und letztendlich ist zu berücksichtigen, dass nur die Existenz eines wirksamen Schutzinstruments gegen unberechtigtes Kopieren und Weiterverbreiten Garant dafür ist, dass auch zukünftig elektronische Dokumente wertvollen Inhalts und mit hoher Qualität erzeugt und allgemein erhältlich sein werden.

Gemäß einer bevorzugten Weiterbildung des Verfahrens der semantischen Verschlüsselung ist zudem vorgesehen, dass eine erfindungsgemäß erzeugte Schlüsseldatei (Datenmenge) für Drittpersonen gesondert verschlüsselt (konventionell oder semantisch) wird, und zwar mindestens zweifach, wobei einer ersten Person das Ergebnis der ersten Verschlüsselung und einer zweiten Person das Ergebnis der darauffolgenden zweiten Verschlüsselung zugeordnet wird. Ein derartiges, erfindungsgemäßes Vorgehen hat dann die vorteilhafte Wirkung, dass selbst bei Verlust der eigentlichen Schlüsseldatenmenge die Nutzdatei wieder hergestellt werden kann, indem beide Empfänger der nachfolgenden Verschlüsselungsergebnisse miteinander die zugrundeliegende Schlüsseldatenmenge durch aufeinanderfolgendes Entschlüsseln erzeugen. Ein derartiges Vorgehen, was insoweit einem Vier-Augen-Prinzip entspricht, würde in erfindungsgemäß vorteilhafter Weise die vorliegende Erfindung unabhängig vom Originalschlüssel, nämlich der zuerst erzeugten Schlüsseldatenmenge, machen können und insoweit Unglücksfällen, wie dem Verlust des Originalschlüssels etwa durch Versterben eines Passwortinhabers, vorbeugen können. Entsprechend ist ein zusätzliches, zweifaches Verschlüsseln der korrekten Schlüsseldatei vorgesehen, ein erstes Ergebnis des zusätzlichen Verschlüsselns wird einer ersten Drittperson zugeordnet, ein zweites Ergebnis des zusätzlichen

Verschlüsselns wird einer zweiten Drittperson zugeordnet und die korrekte Schlüsseldatei ist durch aufeinanderfolgendes Entschlüsseln mit dem ersten und dem zweiten Ergebnis wiederherstellbar.

Nicht nur in diesem konkreten Beispiel zeigt sich zudem, dass im Rahmen der Erfindung die so verschlüsselte Nutzdatei eine Volumendatei ist, also -- gegenüber dem offenen Inhalt -- einen vergleichbaren oder allenfalls wenig veränderten Volumenumfang aufweist.

Eine vorteilhafte Realisierungsform der vorliegenden Erfindung liegt darin, die erfindungsgemäße Schlüsselspeichereinheit (Schlüsseldatenbank) lokal vorzusehen, also innerhalb der räumlichen Grenzen der Datenverarbeitungsvorrichtung (z. B. als zusätzliche Festplatte oder anderes, räumlich von dem Dateiablagesystem getrenntes Medium, oder aber logisch-strukturell getrennt, etwa in Form einer anderen Partition mit eigener Laufwerkskennung auf einer gemeinsamen Festplatteneinheit).

Konkret ist es daher beispielsweise möglich, die Volumendaten (als ursprüngliche Datenmenge) über einen Laufwerksbuchstaben in der Art eines Filesystems zu adressieren und anschließend auf die Schlüsseldatenbank zuzugreifen, und/oder die Schlüsseldatenbank in der Art eines hierarchischen Filesystems zu adressieren und etwa mittels eines Laufwerksbuchstabens zu kennzeichnen. Entsprechend ist die Schlüsseldatenbank lokal in der Datenverarbeitungsvorrichtung, jedoch strukturell oder physisch getrennt von einer dem lokalen Dateiablagesystem zugeordneten Laufwerks- oder Massenspeichereinheit vorgesehen, und die Schlüsseldatenbank ist mittels eines eigenen Laufwerksbuchstabens, eines Laufwerkobjektes (mit Datenbankfunktionalität verbunden) od.dgl. in der Art eines Filesystems adressierbar.

Im Ergebnis führt damit die vorliegende Erfindung zu einem deutlich erhöhten Maß an Datensicherheit, insbesondere im Hinblick auf eine ansonsten mit geringem Aufwand durch unautorisierte oder widerrechtlich handelnde Personen mögliche Kopie (Backup) gesamter Filesysteme oder Teile von diesen. Durch die mittels der vorliegenden Erfindung realisierte, bidirektionale lokale Verschlüsselung entstehen nutzbare -- und damit auch für Dritte erst wertvolle -- Daten und Informationen im Zeitpunkt der Abfrage bzw. existieren nur vor dem Ablegen in das Dateiablagesystem, so dass die vorliegende Erfindung auch als grundsätzliche Modifikation eines herkömmlicherweise offenen File-Handlingsystems hin zu einem in beide Richtungen (bezogen auf einen lokal zugeordneten Massenspeicher) durch Verschlüsseln geschützten System verstanden werden kann.

Wesentlicher Vorteil des erfindungsgemäßen Verschlüsselungsverfahrens, im vorliegenden Text auch als "semantische Verschlüsselung" bezeichnet, ist es zudem, dass hier aktive Daten in Form einer beliebigen Verknüpfungsfunktion zur Verschlüsselung herangezogen werden können, insoweit gibt also dieser Schlüssel unmittelbare Eigenschaften des ver- oder entschlüsselten Dokuments (z.B. Reihenfolge oder Lücken) wieder. Dagegen sind klassische Verschlüsselungsfunktionen, die -- eindeutig und konkret -- eine Beziehung zwischen Schlüssel und zu verschlüsselndem Dokument herstellen, eher passiv, d.h. die Verschlüsselungsfunktion bzw. -operation besitzt keine Beziehung zum Dokument.

Ein weiterer, potentiell nutzbarer Aspekt der vorliegenden Erfindung liegt darin, dass, im Gegensatz zu klassischen, bekannten Verschlüsselungsverfahren, das Ergebnis der semantischen Verschlüsselung ein elektronisches Dokument sein kann, welches für einen Betrachter bzw. Nutzer einen auf den ersten Blick sinnvollen Charakter haben kann. Entsprechendes gilt für das Entschlüsseln, mit dem Ergebnis, dass prinzipiell jeder Ver- oder Entschlüsselungsvorgang zu einem scheinbar sinnvollen Ergebnis führen kann (demgegenüber ist es etwa bei herkömmlichen Kryptografieverfahren eindeutig, ob ein erfolgreiches Entschlüsseln stattgefunden hat, denn nur dann entsteht auch ein sichtbar sinnvolles Ergebnis). Dies gilt insbesondere für den Anwendungsfall der Erfindung, dass die Schlüsselverwaltungseinheit zum Erzeugen und Zuweisen einer Mehrzahl von nutzerspezifischen und volumendateispezifischen Schlüsseldateien für jede Volumendatei ausgebildet ist, wobei die Schlüsselverwaltungseinheit mit einer als Teil des lokalen Dateiablagesystems, von diesem logisch getrennt vorgesehenen Schlüsseldatenbank verbunden ist und zum Verknüpfen einer in der Schlüsseldatenbank gespeicherten Schlüsseldatei mit einer im lokalen Dateiablagesystem gespeicherten Volumendatei so ausgebildet ist, dass im Fall der Verwendung einer korrekten der Mehrzahl von erzeugten und zugewiesenen Schlüsseldateien das korrekte elektronische Dokument erzeugt wird, und im Fall der Verwendung einer nicht korrekten der gespeicherten Schlüsseldateien ein für einen Nutzer scheinbar korrektes elektronisches Dokument erzeugt wird.

Die semantische Verschlüsselung führt damit zu einer potentiell erhöhten Sicherheit im Umgang mit verschlüsselten oder entschlüsselten Dokumenten, wobei damit zusätzlich die Notwendigkeit entsteht, etwa einem Benutzer nach einer durchgeführten, erfolgreichen Entschlüsselung anzuzeigen, dass er auch tatsächlich das offene, entschlüsselte Ergebnis vorliegen hat, und nicht etwa ein (da ein Entschlüsselungsvorgang erfolglos geblieben ist) nach wie vor verschlüsseltes Dokument.

Eine derartige Anzeige kann etwa durch ein zusätzliches Originalitätssignal erreicht werden, etwa in Form eines (nur) dem Benutzer konkret in dieser Bedeutung bekannnten, optischen Hinweises.

Eine zusätzliche Qualität erhält die im Rahmen der vorliegenden Erfindung eingesetzte semantische Verschlüsselung weiterbildungsgemäß dadurch, dass nicht nur die erfindungsgemäß mit den Operationen Vertauschen, Entfernen, Hinzufügen oder Austauschen manipulierten Informationskomponenten zu Verschlüsselungszwecken herangezogen werden, sondern eine Verschlüsselungswirkung zusätzlich dadurch erreicht wird, dass die in der durch semantische Verschlüsselung erzeugten Schlüsseldatenmenge vorliegenden Angaben über die vertauschten, entfernten, hinzugefügten und/oder ausgetauschten Informationskomponenten selbst Operationen des Ver- oder Austauschens unterzogen werden. Mit anderen Worten, die Weiterbildung der semantischen Verschlüsselung liegt in dem semantischen Verschlüsseln der einem jeweiligen Dokument zugrunde liegenden sprachlichen / textlichen / strukturellen Metaebene (die selbst als ein Weg zum Beschreiben des elektronischen Dokuments verstanden werden kann). In der konkreten Realisierung würden dadurch also beispielsweise die Angaben (z.B. Befehle oder Syntaxelemente), die den semantischen Verschlüsselungsvorgang beschreiben, ihrerseits durch andere, bevorzugt nicht-sprechende, Angaben ersetzt (mit der Folge, dass vor einem eigentlichen Entschlüsseln erst eine solche Schlüsseldatenmenge wiederhergestellt werden müßte).

Ein konkretes Beispiel für eine derartige, weiterbildungsgemäß im Rahmen der Erfindung ebenfalls verschlüsselungsfähige Metasprache sind sog. TAG-Elemente, wie etwa Formatierungsanweisungen für Tabellen od.dgl. Auch derartige Format- und/oder Strukturelemente eines Dokuments, die, gewissermaßen übergeordnet über den eigentlichen inhaltsgebenden Worten oder Sätzen existieren, sind im Rahmen der vorliegenden Erfindung durch die Basisoperationen des Vertauschens, Entfernens, Hinzufügens oder Austauschens behandel- und damit schützbar.

Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus der nachfolgenden Beschreibung bevorzugter Ausführungsbeispiele sowie anhand der Zeichnungen; diese zeigen in:

Fig. 1: ein schematisches Blockschaltbild der Datenverarbeitungsvorrichtung gemäß einer ersten, bevorzugten Ausführungsform der Erfindung und

Fig. 2: ein schematisches Blockschaltbild einer Schlüsselerzeugungs- und -verwaltungseinheit im Rahmen der Erfindung.

Die Fig. 1 verdeutlicht anhand eines Einplatz-Computersystems, wie die vorliegende Erfindung mit Baugruppen und Komponenten eines handelsüblichen PCs realisiert werden kann.

Eine lokale Recheneinheit 10, realisiert durch das PC-Mainboard mit üblichen Prozessor-, Speicher- und Schnittstelleneinheiten, greift auf ein lokales Dateiablagesystem 12, realisiert als Festplatte, zu, wobei die Verbindung zwischen Recheneinheit und Dateiablagesystem bidirektional ist, also sowohl Schreibvorgänge der Recheneinheit auf das Dateisystem durchgeführt werden können, als auch umgekehrt Dateien der Einheit 12 gelesen (aufgerufen) werden und dann über geeignete Ein-/Ausgabeeinheiten 14 (z. B. ein Bildschirm, Drucker, Schnittstellen zum Anschließen anderer Rechnersysteme, Datenleitungen usw.) offen lesbar bzw. nutzbar zur Verfügung stehen.

Das Dateiablagesystem 12 kann dabei ein logisch-strukturell getrenntes Dateiablagesystem sein, das als Teil einer größeren Dateiablage für den vorliegenden Zweck speziell vorgesehen ist.

Wie die Fig. 1 zeigt, ist zwischen Recheneinheit 10 und Dateiablagesystem 12 eine Schlüssel-Verwaltungseinheit 16 zwischengeschaltet, die eine bidirektionale Verschlüsselung von in Richtung auf das lokale Dateiablagesystem 12 gerichteten, zu speichernden Nutzdateien -- Textdateien, Bilddateien usw. -- vornimmt, und die zudem in entgegengesetzter Richtung eine Entschlüsselung von im lokalen Dateiablagesystem gespeicherten, als solche nicht lesbaren (d. h. nicht brauchbaren) Volumendateien zurück in eine brauchbare Nutzerdatei vornimmt.

Zu diesem Zweck bedient sich die Schlüsselverwaltungseinheit einzelner Schlüssel, die benutzer- (gruppen-) spezifisch sowie dateispezifisch erzeugt werden und in einer Schlüsselspeichereinheit 18 abgelegt sind.

Im beschriebenen Ausführungsbeispiel ist die Schlüsselspeichereinheit physisch auf derselben Festplatte wie das Dateiablagesystem 12 enthalten, jedoch logisch und strukturell von diesem getrennt, indem der Schlüsselspeichereinheit 18 (alternativ oder zusätzlich: dem Dateiablagesystem 12) eine eigene Laufwerkskennung zugeordnet ist.

Erst mittels des dokumentspezifischen Schlüssels ist es für einen Benutzer der Recheneinheit möglich, eine im System 12 gespeicherte Volumendatei in benutzbarer (lesbarer) Weise auszugeben, bzw. eine aktuell bearbeitete Datei dort abzulegen.

Weiterhin sieht die in Fig. 1 gezeigte Ausführungsform der Erfindung vor, dass, mit der Recheneinheit verbunden, eine Benutzer-Identifikationseinheit vorhanden ist, die beispielsweise

durch ein geeignetes Softwaremodul im Rahmen des Rechner-Betriebssystems oder eines konrekten Anwendungsprogrammes realisiert sein kann.

Eine solche Benutzeridentifikation ermöglicht es, die in der Schlüsselspeichereinheit 18 abgelegten Schlüsseldateien benutzerspezifisch zuzuordnen und zur Verfügung zu stellen, so dass auf diesem Wege einem jeweiligen Benutzer der Zugriff nur auf für ihn autorisierte Volumendateien in dem Dateiablagesystem 12 möglich ist. Besonders geeignet enthält beispielsweise im dargestellten Ausführungsbeispiel das für die Schlüsselspeichereinheit vorgesehene Laufwerk eine -- für den Benutzer unsichtbare -- Unterteilung nach Benutzern für jeweils vorgesehene Schlüsseldateien, so dass die Sicherheit des Zugriffs auf das Dateiablagesystem weiter erhöht wird.

Neben gängigen Verschlüsselungsverfahren für im Dateiablagesystem unlesbar (und damit als solche unbrauchbar) gehaltene Volumendateien bietet sich zur Realisierung der vorliegenden Erfindung insbesondere die sog. semantische Verschlüsselung an, also das planmäßige Verändern des Inhalts einer Volumendatei durch etwa das Umstellen der Reihenfolge von Inhaltskomponenten eines nur in dieser bestimmten Reihenfolge sinnvoll und (vollständig) nutzbaren Inhaltes (also etwa ein Umstellen von Wörtern oder Sätzen innerhalb eines Gesamttextes), wobei dann der hierzu generierte und in der Schlüsselspeichereinheit 18 abgelegte Schlüssel eine korrekte Reihenfolgeinformation erhält. Andere Möglichkeiten einer solchen semantischen Verschlüsselung wären das Austauschen, Weglassen oder Ersetzen von vorbestimmten oder zufällig ausgewählten Schlüsselwörtern, das Erzeugen von Lücken oder das Einfügen von sinnentstellenden Zusätzen.

Auf die beschriebene Weise würde somit ein unautorisierter Zugriff auf das Dateiablagesystem, etwa im Wege eines vollständigen Backup, den Zugreifenden lediglich mit unvollständigen und im Ergebnis nutzlosen Daten belassen, die selbst durch gängige Entschlüsselungsverfahren, ohne die getrennt gespeicherte Schlüsselinformation, nicht in lesbare Form herstellbar sind.

Durch die Wirkung der Schlüsselverwaltung im Hintergrund (nach einmal erfolgter Identifikation des Benutzers durch die Einheit 20) bleiben zudem diese sicherheitserhöhenden Vorgänge für den Benutzer unbemerkt, und, insbesondere wenn -- etwa durch Einsatz speziell eingerichteter Hardware-Bausteine für die Schlüsselverwaltungseinheit 16 -- die Ver- und Entschlüsselungsschritte schnell genug ablaufen, wirkt sich das erfindungsgemäße Vorgehen auch hinsichtlich der konkreten Betriebsgeschwindigkeit des Datenverarbeitungssystems nicht nachteilig aus.

Im Rahmen der vorliegenden Erfindung liegt es zudem, die eins-zu-eins-Beziehung von Volumendatei und Schlüsseldatei dahingehend zu modifizieren, dass insbesondere auch einer (z. B. besonders umfangreichen) Volumendatei eine Mehrzahl von Schlüsseldateien zuzuordnen ist, wobei in diesem Fall der Begriff "volumendateispezifisch" im Hinblick auf jeweilige Dateiabschnitte bzw. Bereiche für eine zugehörige Schlüsseldatei zu interpretieren ist.

Im weiteren soll beschrieben werden, wie die Ausführungsform gemäß Fig. 1 von einem -- autorisierten oder unautorisierten -- Benutzer in der Art eines Filesystems zugegriffen werden kann, so dass die Art und Weise des Zugriffs selbst Bestandteil der Sicherheitsstruktur der vorliegenden Erfindung wird.

Wesentliche Aufgabe der Schlüsselverwaltungseinheit 16 ist das Herstellen einer logischen Beziehung zwischen Volumendaten 12 und jeweiligen (benutzer- und dokumentspezifischen) Schlüsseldaten 18. In einer bevorzugten Realisierungsform der Erfindung läßt sich dabei insbesondere die Kombination von Schlüsselverwaltungseinheit 16 und Schlüsselspeichereinheit 18 als programmtechnisch zu lösende spezielle Darstellungsform zu verstehen, die, etwa in der Art des Explorer für das Windows-Betriebssytem, in der Lage ist, individuelle (d.h. benutzerspezifische, abhängig von einer jeweiligen Autorisierung) Ansichten von elektronischen Dokumenten in einer hierarchischen Anordnung darzustellen, wie es der Dateiordnung und der jeweiligen Berechtigung des Benutzers entspricht. Mit anderen Worten, durch Wirkung der Einheit 16 erhält der Benutzer als Ansicht (und auch zum Zugriff) eine hierarchische Anordnung von für ihn autorisierten Dokumenten dargestellt, im Idealfall so, dass er den Umstand einer Verschlüsselung der jeweiligen dargestellten Dokumente (bzw. einer Nicht-Verschlüsselung) nicht bemerkt. Er kann also innerhalb dieser individuellen, benutzerspezifischen, durch einen Autorisierungsvorgang bestimmten Ansicht so agieren, als würden keine Schutzmechanismen sichtbar existieren.

Gleichwohl basiert eine derartige, aus Benutzersicht (nach wie vor komfortable) Möglichkeit der Arbeit mit der vorliegenden Erfindung auf einer übergeordneten, sicheren Zuordnung und Dokument- bzw. Schlüsselverwaltung, wie sie die eigentliche Aufgabe der Einheit 16 ist: Mit Hilfe typischerweise eines Datenbanksystems, im einfachsten Fall einer Konkordanztabelle, welche verschiedenen Personen die jeweils für sie autorisierten Volumendateien, Schlüsseldateien, zugehörige Attribute usw. zuordnet, ist die in der Einheit 16 enthaltene Darstellungseinheit in der Lage, die benutzerspezifische Ansicht individuell zu kreieren und im Rahmen dieser benutzerspezifischen Ansicht dann auch ggf. verschlüsselte Dokumente mit zugehörigen Schlüsseldateien korrekt zusammenzuführen und so zu rekonstruieren. Ein derartiges, die Funktion der Einheit 16 bestimmendes Datenbanksystem (Beispiel: Tabelle) enthält diesbezüglich typischerweise die den jeweiligen Schlüssel-, Volumen-Dateien zugehöri-

gen Pfadangaben; ergänzend und/oder alternativ können insbesondere auch Rekonstruktionsanweisungen als Bestandteile von Schlüsseldateien unmittelbar in einer solchen Tabelle zum Zugriff enthalten sein (was sich insbesondere dann anbietet, wenn eine derartige Tabelle dynamisch erzeugt wird und der dadurch erhaltene Vorteil ausgenutzt wird, dass das gesamte Dateisystem nicht zusätzlich belastet wird). Insoweit ist als "Schlüsseldatei" im Rahmen der vorliegenden Erfindung insbesondere auch als Eintrag in einer solchen Datenbank (Tabelle) zu verstehen, dergestalt, dass dieser Eintrag das ordnungsgemäße Rekonstruieren im Rahmen der Erfindung ermöglicht. Auch dieser Ansatz bietet Eingriffs- bzw. Ansatzmöglichkeiten für das bevorzugt anzuwendende Schutzverfahren der semantischen Verschlüsselung: Nicht nur kann Aufbau, Feldinhalt und/oder Reihenfolgeposition eines Eintrags innerhalb der Datenbank (Tabelle) semantisch manipuliert sein, auch ist das Vorsehen von Zwischentabellen (etwa in Form von sog. N:M-Zuordnungen) möglich, um Komplexität und damit Entschlüsselungssicherheit der Vorrichtungen weiter zu erhöhen. Zur weiteren Sicherheitserhöhung ist es zudem, analog dem Gedanken der Mehrzahl von Schlüsseldateien zu einem Volumendokument, möglich, mit einer Mehrzahl von (zueinander bevorzugt äquivalenten) Konkordanztabellen zu arbeiten, die, über die Aufgabe der Volumendatei-, Schlüssel- und Personenzuordnung, eine Mehrzahl von möglichen Ansichten bzw. Bearbeitungsbereichen (für jede Person, oder für mehrere Personen) ermöglichen.

Bestandteil der benutzerspezifischen Ansichten bzw. der dadurch gegebenen Bearbeitungsumgebungen ist, durch das Filesystem geregelt, die Möglichkeit einer Anpassung, Aktualisierung bzw. eines Updates für durch Eingriff des Benutzers entsprechend geänderte Inhalte eines jeweiligen elektronischen Dokuments, insbesondere betreffend das Fortschreiben des Verschlüsselungsmechanismus zwischen Volumendatei (in Einheit 12) und Schlüsseldatei (in Einheit 18), so dass auch insoweit der vom Benutzer zugefügte Dokumentbestandteil und/oder dessen Änderung entsprechend Verschlüsselung enthält. Damit sind im Rahmen der vorliegenden Ausführungsform Synchronisationsmechanismen geschaffen.

Auf diesem Wege ist dann insbesondere auch das Abfangen missbräuchlicher Zugriffsversuche auf die Datenverarbeitungsvorrichtung der vorliegenden Erfindung möglich: Erfolgt etwa ein missbräuchlicher Zugriff auf den autorisierten Datenbestand für eine Person (erkannt z.B. dadurch, dass sich ein missbräuchlich Zugreifender zwar für eine Person autorisiert, jedoch ein falsches Passwort eingibt), so erhält dieser Zugreifende zwar durch Wirkung der Schlüsselverwaltungseinheit 16 eine Ansicht von Dateien dargeboten, ist jedoch weder in der Lage, auf den tatsächlichen, vollständigen Inhalt dieser Dateien zuzugreifen, noch wird es ihm ermöglicht, Änderungen an diesen Dateninhalten vorzunehmen. Vielmehr ist das System so ausgebildet, dass es auf Eingaben des Zugreifenden reagiert, insoweit also entsprechenden Änderungen folgt, diese schlagen sich jedoch nicht in den erfindungsgemäß geschützten Ori-

ginaldaten wieder, sondern nur in der durch die Einheit 16 verwalteten virtuellen Sicht des widerrechtlich Zugreifenden. So können zwar durch Eingriff eines widerrechtlich Zugreifenden durchaus verschlüsselte Volumendaten geändert werden (woraufhin dann eine entsprechende Anpassung der Schlüsseldaten erfolgt), das zugrundeliegende, ursprüngliche Dokument bleibt jedoch von diesen Manipulationen unbeeinflusst.

Auf die oben beschriebene Weise stellt sich daher somit die Schlüsseldatenbank bzw. die Schlüsselverwaltungseinheit als Bestandteil der erfindungsgemäßen Datenverarbeitungsvorrichtung dar, die logische und damit virtuelle, hierarchisch geordnete und individuell - benutzerspezifische Ansichten (und damit Benutzer-Zugriffsbereiche auf der lokalen Rechnereinheit) schafft, die jedoch gleichermaßen einen Maximum an Zugriffsschutz gegen missbräuchlichen Zugriff sicherstellt, indem nämlich, insbesondere mit dem Instrument der semantischen Verschlüsselung, ein tatsächlicher Zusammenhang zwischen Schlüsseldateien (mit Rekonstruktionsanweisungen) und einer zugrundeliegenden Volumendatei unsichtbar und intransparent bleibt.

In der praktischen Realisierung der vorliegenden Erfindung erscheint es dabei insbesondere auch ratsam, sehr weitgehend vom Betriebssystem vorgesehene Operationen des Dateizugriffs an die erfindungsgemäße Vorgehensweise anzupassen, nicht zuletzt um eine ordnungsgemäße Unterscheidung von erfindungsgemäß zu sichernden und ansonsten offenen, frei zuzugreifenden Dateien eines eher typischerweise für verschiedene Anwendungen benutzten lokalen Rechnersystems sicherzustellen, ohne dass Sicherheitslücken auftreten (oder dass, von autorisierten Zugreifenden, verschlüsselter Volumendaten irrtümlich als unverschlüsselte Originaldaten missinterpretiert werden, was durch den Charakter der semantischen Verschlüsselung ohne weiteres gegeben sein könnte). Da jedoch derartige Eingriffe in ein Betriebssystem problematisch sein könnten, wäre es alternativ möglich, im Rahmen der vorliegenden Erfindung überhaupt betroffene Dateien mit einem Header zu versehen, welcher obligatorisch und automatisch eine Überprüfung auslöst, ob es sich um eine bestimmungsgemäß zu verschlüsselnde bzw. im Rahmen der vorliegenden Erfindung zu behandelnde Datei handelt, oder aber um eine prinzipiell unverschlüsselte.

Dementsprechend liegt eine weitere, mögliche Weiterbildung der vorliegenden Erfindung darin, mit Mitteln des Datenbank- und Systemdesigns der vorliegenden Datenverarbeitungsvorrichtung die Grenzen zwischen Benutzern individuell, selektiv anzuzeigenden (und zuzugreifenden) elektronischen Dokumenten und solchen Dokumenten, die irgendwelchen Zugriffsregeln überhaupt nicht unterliegen, verwischen zu lassen (also die Ansichten auf die Verzeichnisse und der darin enthaltenen Dokumente nicht zu trennen) und insoweit Unsicherheit

darüber entstehen zu lassen, ob überhaupt die innerhalb einer benutzerspezifischen Ansicht dargebotenen elektronischen Dokumente zugriffsgeschützt sind.

Darüber hinaus liegt eine vorteilhafte Weiterbildung der vorliegenden Erfindung darin, die gemäß der vorbeschriebenen Ausführungsformen verwendeten, benutzerspezifischen Ansichten der Dateien im Filesystem dynamisch und insbesondere im Zusammenhang mit einem jeweiligen Beginn einer Benutzersession eines Benutzers überhaupt erst zu erzeugen, so dass insoweit ein festes, invariables Schema von benutzerspezifischen Ansichten überhaupt nicht existiert (entsprechend auch auf einer Überwachungs- bzw. Supervisorebene nicht kontrollierbar, sogar explizit abkoppelbar ist), und so der Sicherheitscharakter der Gesamtlösung weiter verstärkt wird.

Zur ergänzenden Erläuterung des Verschlüsselungsverfahrens gemäß unabhängigem Anspruch 8 (im weiteren auch "semantische Entschlüsselung" genannt), werden im folgenden Details und Eigenschaften dieses Verfahrens näher beschrieben, die Gegenstand der vorliegenden Erfindung sind.

Die semantische Verschlüsselung, also die Verschlüsselung des Sinns besteht in der Aufteilung von Originalen Daten (OD) in Volumendaten (VD) und Arbeitsanweisungen oder Rekonstruktionsanweisungen (RA). Es liegt in dem zugrundeliegenden Konzept des Verfahrens, daß die Volumendaten frei und ohne zusätzlichen Schutz verteilt werden können. Die RA müssen getrennt von den VD aufbewahrt werden. Die Benutzung der OD und der Zugriff auf die OD geht nur, wenn der Zugriff auf die RA mit Reglementierungen belegt sind und die RA entsprechend geschützt abgespeichert sind und auf sie nur reglementiert zugegriffen werden kann.

Die Verwaltung der RA bzw. der Schlüsseldaten und des Zugriffs auf diese RA geschieht durch eine Datenbank, im folgenden auch Schlüsseldatenbank oder Schlüsseleinheit genannt. Da der Zugriff auf diese zentrale Schlüsseleinheit ebenfalls mit einem Schlüssel und / oder mit einem Paßwort geschieht und da diese Daten besonders sensibel sind und daher das erste Ziel von Angriffen auf die Vertraulichkeit und auf die Geheimhaltung der darin enthaltenen Daten darstellt, muß die Sicherheit vor unautorisierten Zugriff durch eine zusätzliche Verschlüsselung sichergestellt werden.

Diese Schlüsseleinheit erlaubt die Abspeicherung der Zugriffsdaten oder Zutrittsdaten (ZD) und bietet damit den Zugriff auf die Daten im Rahmen einer Zugriffskontrolle.

Bei einem Zugriff will ein Benutzer also ein Subjekt auf ein OD Objekte zugreifen. Ob überhaupt die Rechte für die beabsichtigte Zugriffsoperation vorhanden sind, entscheidet die Zugriffskontrolle.

Die Zugriffskontrolle entscheidet, ob die angefragte RA für ein identifiziertes Subjekt freigeschaltet werden darf, oder ob die Übergabe der RA an dieses Subjekt blockiert werden muß.

Der Zugriffsschutz auf das Dokument besteht somit aus einer semantischer Verschlüsselung des Dokumentes auf einem Massenspeichers und aus einer klassisch oder semantisch verschlüsselten Zugriffs auf die RA, die zu den semantisch verschlüsselten VD gehört.

Die Daten in der Schlüsseleinheit können ebenfalls bei einem Backup mit abgespeichert werden. Der Zugriff auf die Daten innerhalb dieses Schlüsseleinheit kann zusätzlich erschwert werden, wenn der Schlüssel mit dem auf den Schlüsselserver zugegriffen werden kann, nicht eindeutig ist. Wenn mehr als ein Schlüssel für die Entschlüsselung plausibel oder gar nur theoretisch möglich ist, dann bedarf es zusätzlicher Kriterien, um sich selber und andere davon zu überzeugen, daß der Schlüssel korrekt ist.

Der Nachteil der klassischen Kryptographie besteht darin, daß die natürlichen Redundanz der Sprache genutzt werden kann, um die verwendeten Schlüssel berechnen zu können, oder daß die Schlüssel sofern sie vorliegen genutzt werden können um durch einmalige die Anwendung sehr leicht beweisen zu können, daß sie korrekt sind. Der Beweis, daß der gegebene Schlüssel eindeutig ist, kann durch statistische Verfahren bei größeren Datenmengen leichter geführt werden. Je größer die Datenmenge ist, desto leichter ist auch die Entschlüsselung.

Der Vorteil der semantischen Verschlüsselung besteht außerdem darin, daß besonders große Datenmengen zuverlässiger und sicherer geschützt werden können. Die semantische Verschlüsselung liefert eine sehr große Menge von möglichen Schlüsseln, die angewandt auf Volumendaten sinnvolle und ggf. auch brauchbare Daten liefern. Auch ein amateurhafter Angreifer könnte sich selber eine ganze Klasse von Schlüsseln ausdenken, die angewandt auf die verschlüsselten Daten scheinbar einen korrekten Inhalt liefern. Der Beweis von Originalität kann ggf. auch später und unabhängig von der Ver- und Entschlüsselung geführt werden.

Als Beispiel kann der Satz dienen: Holen Sie Herrn Manfred Schmidt morgen (Datum) um 12:17 von Bahnhof in München ab. Obwohl die Ort, die Zeit und der Aktion genau spezifiziert worden ist, kann bei einer semantischen Verschlüsselung keine Aussage darüber getroffen werden, was der originale Inhalt darstellt. Jeder kann Rekonstruktionsanweisungen entwikkeln, mit der der Sinn dieses Satzes geändert werden kann. So kann das Datum, die Uhrzeit,

der Ort die Namen der Personen oder die Aktion z.B. durch das Wort „nicht„ vor dem Wort „ab„ in das genaue Gegenteil umgedreht werden.

Der Beweis der Originalität kann z.B. darin bestehen, daß ein zwischen dem Erzeuger und dem Benutzer dieser verschlüsselten Daten ein Kriterium vereinbart werden kann, daß beide als ein Beweis für Originalität akzeptieren würden. Dieses Kriterium kann anders als bei der klassischen Kryptographie nicht mathematischer und/oder statistischer Art sein. Falls der Erzeuger und Benutzer ein und dieselbe Person ist, so kann z.B. die Signalisierung der richtigen Entschlüsselung in der Anzeige eines vorher nur ihm als korrekt bekannten Bildes darstellen. Ein Angreifer würde ebenfalls immer ein Bildes sehen, aber er könnte nicht wissen, welches und ob es korrekt ist.

Ein in der Schlüsseleinheit verwaltetes mathematisches Kriterium, wie das einer digitalen Signatur, könnte angewandt auf einen im Kontext nicht ersichtlichen Daten Teilbestandes die Zuverlässigkeit des Gesamtsystems für die Benutzer erhöhen, ohne daß daraus Informationen über einen Angriff auf den Schlüssel gewonnen werden kann.

Die Vorteile einer auf ein Datenbankmodell und Verschlüsselung gestützten Zugriffskontrolle besteht in der Herstellung der Sicherheit der Daten, der Nachweisführung, ob Zugriff auf Daten genommen worden ist, das Nachvollziehen und die Überprüfung der Verantwortlichkeit, ob ein Zugriff genommen werden darf und ob eine Änderung an den Daten vorgenommen werden darf. Außerdem kann der Lebenszyklus eines Dokumentes, d.h. das Publizieren eines Dokumentes genauso wie das nicht mehr zugänglich machen eines Dokumentes durch den Zugriffsschutz auf die RA hergestellt werden.

Der Zugriff auf die Backupdaten kann auch über die mitgesicherte Schlüsseleinheit geschehen. Die Schlüsseldaten können so verwaltet werden, daß ein Auslesen dieser Daten und ein Verwalten in einer anderen Schlüsseleinheit verhindert werden kann. Durch den Vergleich der abgespeicherten relativen oder absoluten Datenposition innerhalb des Massenspeicher von der Schlüsseleinheit kann die Zugriffskontrolle innerhalb der Schlüsseleinheit feststellen, ob der Zugriff von einem Backup erfolgt oder von der originalen Schlüsseleinheit.

Über die Zugriffskontrolle können verschiedene Stufen der Geheimhaltung realisiert werden. Da die Dokumente mehr oder weniger unabhängig von der Art der verwendeten semantischen Verschlüsselung nahezu als äquivalent geschützt angesehen werden können, kann die Geheimhaltung der Daten und deren Zugang nur über die Schlüsseleinheit gestaltet werden.
Durch die Zugehörigkeit zu einer Schnittmenge von Benutzergruppen kann einem Teilnehmer die Verwendung eines nur in der Datenbank enthaltenen Zusatzschlüssels ermöglicht werden,

der dann den entschlüsselten Zugriff auf die dokumentenspezifisch und benutzergruppenspezifisch verschlüsselten Daten freigibt.

Der Einsatz der semantischen Verschlüsselung bei der Übertragungssicherung im Rahmen einer Kommunikation besteht in dem Austausch von verschlüsselten Daten zwischen mindestens 2 Teilnehmern A und B. Der Schutz eines Backup oder eines langfristig angelegten Archivs ist ein von der zeitlichen Dauer her betrachteter Übertragungsvorgang als extremes Beispiel für die Anwendung der Übertragungssicherheit anzusehen, da bei der Entwendung des Backup alle nichtgeschützten Daten einem nichtautorisierten Teilnehmer bekannt werden. Bei der Übertragung von Daten muß daher auch zwischen einer synchronen Benutzung von Daten beim Teilnehmer B und von einer späteren also asynchronen (Teil-) Benutzung von übertragenen Daten unterschieden werden. Bei einem Backup wird von einer asynchronen Benutzung der Daten ausgegangen, die außerdem so abgespeichert sein sollten, daß ein Zugriff auf die verschlüsselten Daten jederzeit und mehrfach auch ohne Kenntnis vom Teilnehmer A durchgeführt werden kann.

Bei der Herstellung von Übertragungssicherheit muß es aber mindestens einen Kontakt zwischen A und B gegeben haben, damit eine Identifikation und Authentifikation (I&A) durchgeführt werden kann. Die Übertragung der VD geschieht in einen oder mehreren Datenübertragungsschritte. Die Übertragung der RA kann vor/nach/während der I&A und oder der Übertragung der VD geschehen. Im Rahmen der Erfindung kann die einmalige oder mehrmalige Übertragung der RA der Übertragungssicherheit und der Situation angepaßt werden. Die bei dem Backup auch abgespeicherte Schlüsseleinheit verwaltet über die Zugriffskontrolle den Zugriff auf das Backup.

Falls aufgrund der Anwendung keine Zeitverzögerung bei der Übertragung akzeptiert werden kann, müssen VD und RA zeitlich korreliert übertragen werden. Falls die Anwendung asynchron zur Übertragung mit den OD arbeiten soll, dann kann die Übertragung der RA auch nichtkorreliert geschehen und ggf. auch mit den VD zusätzlich semantisch oder klassisch verschlüsselt mitgegeben werden.

Unter Übertragungssicherheit kann allgemein der Schutz der Vertraulichkeit oder der Schutz vor Veränderungen bei der Übertragung der Daten verstanden werden. Bei der Semantischen Verschlüsselung ist der Schutz der Vertraulichkeit bei VD unmittelbar gegeben. Die Anwendung von zusätzlichen klassischen Verschlüsselungen ist auf eine geringe Anzahl von Daten, z.B. auf die sessionweise, individuell verschlüsselten RA, beschränkt.

Die unbemerkte Änderung der auszugebenden entschlüsselten Daten, kann bei der Änderung der VD nur unterhalb einer von dem Angreifer nicht erkennbaren Auflösung geschehen, falls z.B. die Rekonstruktion nur in der Wiederherstellung der richtigen Reihenfolge von Sätzen bestehen würde. Da z.B. die Semantische Verschlüsselung nur in der Änderung der Reihenfolge der Sätze bestehen könnte, kann die Änderung von Wörter innerhalb eines Satzes nicht festgestellt werden. Für die Registrierung einer Änderung ist der Augenschein nicht ausreichend. Daher kann ein zusätzliches Verfahren zur digitalen Beweissicherung für die Feststellung von Änderungen bei den Volumendaten eingeführt und mit der semantischen Verschlüsselung kombiniert werden.

Wenn die Volumendaten bei der Kommunikation als ganzes oder als verwendbare Teildaten komprimiert sind, dann kann die Übertragung der Daten schneller und auch zuverlässiger erfolgen. Die Sicherheit der so übertragenen Daten ergibt sich aus der nichtlinearen Verknüpfung zwischen den komprimierten Daten. Dagegen kann die heruntergeladene komprimierte Datei auf dem lokalen Rechner in der oben beschriebenen Weise verändert werden, so daß für die Verhinderung dieser Manipulationen auch klassische Methoden der Beweissicherung ihre Anwendung finden können.

Bei einem Verwendungszweck in der Beweissicherung steht im Vordergrund, ob die Daten echt sind, d.h. im Sinne originär, unverändert oder unversehrt vorliegen. Die Daten sind von einem bestimmten (anonymen oder bekannten) Benutzer, sie stammen von einer bestimmten Quelle, bzw. sind an einem bestimmten Datum erstellt worden. Bei der Beweissicherung muß ggf. der Kontext der Daten dargestellt werden. Zu dem Kontext können auch die Zugriffsdaten gehören. Für die Beweissicherung muß nachvollzogen werden können, daß die Volumendaten, die RA und die Datenbank, auf der die Zugriffsdaten abgespeichert sind, nicht verändert worden sind bzw. nicht ohne Spuren zu hinterlassen verändert werden können.

Bisher konnte die Beweissicherung nur mit einer der folgenden Mittel hergestellt werden: Abspeicherung des Wertes einer Einwegfunktion, d.h. Verwendung einer digitalen Signatur oder die Abspeicherung der Daten auf ein nicht mehr veränderbares Speichermedium (Laserdisc, WORM) auf die zu schützenden Elemente (VD, RA, ZD und Datenspeichereinrichtung). Als zusätzlicher Vorteil der semantischen Verschlüsselung wirkt sich die Trennung der OD in VD und RA als eine zusätzliche Verbesserung der Sicherheit der bestehenden Verfahren zur Beweissicherung aus. Die Beweissicherung ist im Rahmen der Semantischen Verschlüsselung ein unabhängiges Add-On, auf das je nach Anwendung auch verzichtet werden kann, und als Teil der Schlüsseleinheit angesehen werden kann, bei der jede zusätzliche Verschlüsselung sich relativ zu dem bestehenden Datenkontext hinzufügt.

Da die Positionierung von Daten sich relativ zu einer Menge von sich ändernden Orientierungsmarken innerhalb eines Datenkontext verändern kann, kann neben der Entschlüsselung der Daten auch das Änderungsprotokoll als relative Aktualisierungsdaten semantisch verschlüsselt abgespeichert werden. Eine Manipulation in der abgespeicherten Vergangenheit dieser Daten würde so sofort registriert werden können, da der Kontext entweder von der Gesamtdatei oder von einer Teildatenmenge zerstört werden kann.

Der Vorteil der semantischen Verschlüsselung besteht darin, daß kein inhärenter Integritätsschutz enthalten ist und daß er durch zusätzliche Verfahren gezielt mit Redundanz oder mit anderen Kontext schaffenden Informationen zusätzlich herangeführt werden kann.

Die Überprüfbarkeit von Datenintegrität, also die Feststellung einer Änderung von Daten, die entweder bei der Quelle (Server), bei der Übertragung oder auf dem lokalen Rechner manipuliert worden sein kann, ist für die Vertrauenswürdigkeit der semantisch verschlüsselten Daten wichtig. Die Datenintegrität ist für die Anerkennung von Daten durch den Benutzer wichtig. Zu diesem Zweck kann ein mathematisches Beweisführungsverfahren, wie die Anwendung einer Einwegfunktion zusammen mit einer lokalen Datei oder ein unverändertes Merkmal auf einem Server bei dem entsprechenden Nachweis eingesetzt werden.

Bei einer Überprüfung der Datenintegrität findet entweder diese Überprüfung auf der lokalen Maschine oder auf dem Server geschehen, je nachdem wie die Interessen bei dieser Überprüfung verteilt sind. Eine Änderung der Daten kann durch die mathematischen Beweisführungsverfahren jederzeit, also auch vor der unmittelbaren Benutzung durch den Anwender durchgeführt werden.

Eine semantische Überprüfung der Datenintegrität kann flexibel durch eine Metasprache vorgenommen werden, bei der sich die semantische Ver- und Entschlüsselung flexibel durch eine minimal geänderte Metasprache drastisch im rekonstruierten Ergebnis auswirkt, so daß die Korrektheit des Schlüssels durch die Betrachtung der so rekonstruierten Daten relativ einfach durch Augenschein erkannt werden kann.

Für die Beweissicherung und Datenintegrität ist die Authentizität wichtig und nicht die Geheimhaltung der so überprüften Daten. Die Geheimhaltung ergibt sich aus der zusätzlichen Verschlüsselung der Daten. Ob die Datenintegrität vor oder nach der Verschlüsselung geprüft wird ergibt sich aus der konkreten Anwendung.

Bei der Schlüsselverwaltung ist zu differenzieren in Bezug auf den Schlüssel als Paßwort zur Identifizierung und Authentifizierung, im folgenden nur Paßwort genannt, und Schlüssel als

Rekonstruktionsanweisung für die Elektronischen Dokumente. Die Schlüssel können dabei selber Anweisungen enthalten, die wiederum komplexere Verschlüsselungsoperationen auslösen können, und die sich dabei ggf. in eine Menge von Schlüssel umwandeln.

Die Schlüssel können auch nur temporär für eine Kommunikation oder für eine Menge von Kommunikationsschritten, z.B. für eine Benutzersession, eingesetzt werden. Die Abspeicherung der RA in der Datenbank kann auch zusätzlich verschlüsselt werden. Die Verwendung von Schlüssel (im Folgenden RA-Schlüssel genannt) kann dabei für eine Mengenbildung innerhalb der so verschlüsselten Daten verwendet werden. Mit einem RA-Schlüssel können dann beispielsweise alle RA für ein Dokument oder alle RA für ein Kapitel mit allen darin enthalten Versionsänderungen verschlüsselt werden.

Verschlüsselt wird stets eine ursprünglichen Datenquelle, die mit einer definierten Vokabular aufgebaut wird. Alle Sprachen, insbesondere die natürlichen menschlichen Sprachen, bestehen aus einer Menge von Wörter, die in einem Lexikon aufgelistet werden können. Die Anwendung im Rahmen von kontextbezogenen Sätzen können Wörter noch konjugiert und dekliniert werden.

Die Verwendung von falschen grammatischen Formen ist innerhalb der schriftlichen und mündlichen Sprache üblich und wird von Menschen in der Regel richtig interpretiert sofern es nicht deutlich oberhalb einer Reizschwelle liegt und oder zu Mißverständnissen, Unklarheiten oder zu Konflikten mit der Kontext steht und zu Sinn behafteten Irritationen führt.

Die Verschlüsselung eines Backup hat ein zusätzliches Problem, daß bei einer Datenübertragung keine äquivalente Bedeutung hat. Da Backup Bänder und deren ggf. illegal gemachte Kopie sehr lange aufbewahrt werden können, besteht einerseits das Problem ein Zugriffspaßwort zu haben, daß auch nach Jahren wieder erinnert und verwendet werden kann, andererseits besteht das Problem, daß die Endtarnung des Paßwort weitreichende Folgen für die Datensicherheit hat. Wenn die Paßwörter zu schwierig zu merken sind, dann besteht die Gefahr des Vergessens. Wenn dagegen das Paßwort für den Hersteller des Backup oder eines Benutzer, dessen Daten abgespeichert werden, sehr leicht zu merken ist, dann stellen klassische Verschlüsselungsverfahren keine Schutz mehr dar. Dagegen würde eine semantische Verschlüsselung der Schlüsseleinheit keine Hinweise oder Beweise liefern, daß der einfache Schlüssel tatsächlich der richtige Schlüssel ist.

Die Verwendung einer lokalen Schlüsseleinheit erspart dem Benutzer umfassende Ausfallmaßnahmen zu treffen, für den Fall, daß der Schlüsselserver ausfällt. Die flexiblere Verteilung

der Schlüssel ermöglicht eine Online Zugriff auf einen externen ggf. zentral verwalteten Schlüsselservers, für den Fall einer zusätzlichen Abgleich zur Herstellung der Aktualität.

Ein weiterer Fortschritt besteht in der Begegnung der Gefahr, daß auch in einer zentralen Datenbank eingedrungen werden kann und daß die Kenntnis aller Schlüssel zu einem entsprechend großen Schaden führen kann. Außerdem besteht das Problem in einer möglichen Überlastung durch zu viele Anfragen auf eine zentralen Datenbank, was zu Problemen in der effizienten ökonomischen Ausnutzung von Ressourcen führen kann.

Bei einer Schlüsselverteilung muß berücksichtigt werden, ob der Schlüssel geholt werden muß oder verschlüsselt geliefert wird, oder bereits durch das Paßwort lokal vorhanden ist. Außerdem kann unterschieden werden, ob die Schlüssel bzw. die Paßwörter in der Schlüsseleinheit im Klartext eingetragen sind oder von der Schlüsseleinheit zur Überprüfung angefordert werden muß. Die RA Schlüssel können zentral, lokal oder dezentral verteilt gespeichert werden. Die Art der Schlüsselverteilung ergibt sich daraus, ob der Schlüssel symmetrisch oder asymmetrisch ist und ob der Schlüssel nur einmal verwendet werden soll und damit immer neu geholt werden muß. Außerdem ergibt sich das Problem der Schlüsselverteilung aus der Notwendigkeit zur Änderung und zum periodischen Wechseln von Schlüsseln und Paßwörter.

Ein weiterer Vorteil der semantischen Verschlüsselung besteht darin, daß bei einem Wechsel des Schlüssels keine zuverlässige Aussage darüber gemacht werden kann, ob es sich um eine veränderte Verschlüsselung handelt, oder um eine bewußte verändernde Aktualisierung des Datenbestandes. Der Unterschied besteht darin, daß bei einer klassischen Verschlüsselung und bei Kenntnis des entschlüsselten Textes durch eine Klartext auch der neue Schlüssel enttarnt werden kann. Die Gefahr einer Klartext Attacke besteht bei der semantischen Verschlüsselung nicht, da für einen so gefundenen Schlüssel keine Beweis vorhanden ist, daß er richtig ist und daß damit ein darüber hinausgehender Verlust an Vertraulichkeit verbunden ist.

Die Sicherheit der Paßwort Verwaltung ergibt sich zum einen aus der verwendeten Einwegfunktion und zum Anderen aus der Auswahl des Paßwortes durch den Benutzer. Der Vorgabe einer Länge und einer Auswahl aus einem möglichst großen Zeichenvorrat verbessert die Qualität eines Paßwort. Um das Erraten von Paßwörter zu erschweren werden Ausschlußlisten gebildet. Die Paßwortverwaltung ist wie eine Schlüsselverwaltung. Im Gegensatz zu RA Schlüssel werden die Paßwörter in der Regel vom Benutzer festgelegt. Außerdem können sie von diesem eingegeben oder bei Bedarf geändert werden.

Um den Zugriff auf das Backup zu erschweren, kann die Freischaltung der Schlüsseleinheit, die vom Backup geholt worden ist erst dann korrekt arbeiten, wenn eine zusätzliche Informa-

tion von einem vertrauenswürdigen und Rechner geholt wird, der ggf. nur für diesen Zweck bereitwillig Informationen sammelt, aber Antworten erst nach Überwindung mehrerer Einzelschritte ggf. auch organisatorischer Art freigibt.

Die Schlüsseleinheit stellt aufgrund der wichtigen Bedeutung für die Sicherheit der Daten innerhalb der Gesamtlösung ein wichtiges Angriffsziel dar. Wenn ein Benutzer sein Paßwort bei der Identifizierung gegenüber dieser Schlüsseleinheit preisgibt, dann ist damit die Sicherheit des Gesamtsystems ins Gefahr. Aus diesem Grunde muß die Paßworteingabe sich vor sogenannten trojanischen Pferden schützen, die dem Benutzer vorgaukeln, sie wären in Wahrheit die Schlüsseleinheit, aber in Wirklichkeit sind es nur Programme, die den Benutzer dazu verleiten sollen, das Paßwort einzugeben. Dieses Ausspähen des Paßwortes wird auch Spoofing genannt. Die Schlüsseleinheit kann in eine Ausführungsform auch mit zusätzlichen Methoden zur Verhinderung des Spoofing ausgestattet sein, z.B. das Erzeugen einer Mehrzahl von Zugangspassworten für jeden Benutzer (mit vorteilhaft nur einem Korrekten), so dass eine Unsicherheitskomponente bei einem unberechtigt Zugreifenden entsteht.

Die Zugriffskontrolle auf ein Backup kann auch als Kopierschutz Verfahren realisiert werden.

Bei der symmetrischen Verschlüsselung kann von dem Schlüssel zur Verschlüsselung sofort auf den Schlüssel zur Entschlüsselung geschlossen werden. In diesem Sinne kann das Vertauschen und Ersetzen von Daten als symmetrisches Verschlüsselungsverfahren verstanden werden. Durch die Arbeitsanweisung zur Entschlüsselung kann sofort die zugehörige Entschlüsselungs- RA gewonnen werden. In der gleichen Weise ist auch nach der Entschlüsselung gekannt, wie die Verschlüsselung durchgeführt worden ist. Um diese beiden Vorgänge stärker zu trennen, muß eine semantische Zwischenschicht eingeführt werden.

Die Anweisungen zur Vertauschung oder Löschen etc. bestehen aus einem Vokabular oder zumindest aus Token, denen eine definierte Aufgabe zugewiesen wurde. Das Vokabular wird durch die Interpretation der Rekonstruktionseinheit mit einer Aktion verknüpft. Die Interpretation dieses Vokabulars kann man durch die Implementation von ausführenden Operationen einer Metasprache realisieren. Wenn die Zuordnung des Vokabulars zu Operationen wiederum durch eine Metasprache geändert werden kann, so kann ein zusätzlicher Schlüssel genutzt werden, um die Operation der ersten Schlüssels komplexer zu interpretieren. Dieser zusätzliche Schlüssel kann dann entweder dem Sender oder dem Empfänger des RA hinzugefügt werden. Die zusätzlichen Zuordnungen zwischen Vokabular und Operationen können so miteinander funktional interagieren, daß ein zurück rechnen von einen Schlüssel auf den anderen an der Komplexität und Eindeutigkeit des Problems scheitert. Zur Unterstützung dieses Vorgangs können Einwegfunktionen verwendet werden.

Aus dieser Verknüpfung kann auch die semantische Verschlüsselung so eingesetzt werden daß auf deren Basis asymmetrische Verschlüsselung mit all seinen aus dem Stand der Technik bekannten Anwendungen möglich gemacht werden kann.

Message Digits (MD) ergeben sich aus der Anwendung von Einwegfunktionen. Die Anwendung kann auf eine durch die semantische Verschlüsselung vorgegebene Klasse von Entitäten oder auf deren Komplementär Menge beschränkt werden Auf diese Weise können mehrere unabhängige Teil Message Digits entstehen, die jeweils für sich einen Schutz vor zufälligen und absichtlichen Veränderungen bieten. Da MD auf der Byte Ebene angewendet werden und daher für sehr große Datenmengen relativ rechenzeitaufwendig in der Erstellung sind, kann ein semantischer MD auf der semantischen Ebene dazu eingesetzt werden, ob es eine Änderung der Volumendaten oder der Schlüsseldaten oder der Schlüsseleinheit gegeben hat.

Unter Bezug auf die Fig. 2 wird nachfolgend eine praktische Realisierungsform des die Infrastruktur zur semantischen Verschlüsselung betreffenden Aspekts der vorliegenden Erfindung beschrieben.

Die Fig. 2 zeigt dabei in einer schematischen Blockschaltbild-Darstellung den Aufbau einer Schlüsselerzeugungs- und Verwaltungseinheit mit den zugehörigen Funktionskomponenten im Rahmen der vorliegenden Erfindung, die benutzt werden kann, um durch die erfindungsgemäße Technologie der semantischen Verschlüsselung zu schützende elektronische Dokumente in geschützte Volumendateien und zugehörige Schlüsseldateien umzusetzen. Dabei ermöglicht es die im Zusammenhang mit Fig. 2 beschriebene Ausführungsform insbesondere auch, nicht lediglich eine (beim Wiederherstellen zur ursprünglichen, korrekten Datenmenge führende) Schlüsseldatenmenge zu erzeugen, sondern eine Mehrzahl von Schlüsseldatenmengen, so dass auch durch diesen Aspekt des Vorliegens einer Mehrzahl möglicher Schlüssel (von denen auch wiederum nur einer zu dem auch inhaltlich korrekten, und nicht nur scheinbar korrekten Ergebnis führt) die Sicherheit der vorliegenden Erfindung weiter erhöht werden kann.

Die Fig. 2 soll am Beispiel eines elektronischen Textdokuments beschrieben werden, welches in einem üblichen Format (z.B. Microsoft WORD) vorliegt und mit geeigneten Texteditoren erstellt wurde. Das Textdokument besteht aus dem Satz

Peter geht um 20.00 Uhr zum Bahnhof. Der Zug ist pünktlich.

ist in einer Speicherheit 52 gemäß Fig. 2 gespeichert und soll in nachfolgend zu beschreibender Weise durch Wirkung der in Fig. 2 gezeigten, weiteren Funktionskomponenten semantisch verschlüsselt werden.

Eine der Dokumentspeichereinheit 52 nachgeschaltete Lese-/Zugriffseinheit 54, welche mit einer Formatdateneinheit 56 zusammenwirkt, stellt fest, dass das obige, in der Speichereinheit 52 gespeicherte Dokument der Formatstruktur MS-WORD folgt (idealerweise enthält die Formatdateneinheit 56 sämtliche Format- bzw. Strukturinformationen gängiger Datenformate), und greift mit diesen (dateibezogenen) Formatinformationen auf das Textdokument in der Dokumentspeichereinheit 52 zu. Die der Lese-/Zugriffseinheit 54 nachgeschaltete Analyseeinheit 58 ist nunmehr in der Lage, auf der Basis der von der Leseeinheit 54 gelesenen Dokumentinformationen diese zu analysieren und zu bewerten, wobei die Analyseeinheit 58 zum einen das elektronische Dokument in seine einzelnen Informationskomponenten zerlegt und diese in eine Informationskomponentenspeichereinheit 60 ablegt (im vorliegenden Beispiel wären dies die einzelnen Wörter), und zusätzlich die Dokumentstruktur als Struktur von zwei durch Punkte begrenzten Sätzen erkennt und diese Dokumentstruktur in der Dokumentstrukturspeichereinheit 62 zerlegt ablegt. Insoweit erhält der Inhalt der Einheit 62 den Charakter einer dokumentspezifischen Metadatei, auf die auch spätere Verschlüsselungsvorgänge (auch ggf. nur selektiv) zugreifen können.

Konkret könnte der Inhalt der Dokumentstrukturspeichereinheit nach der Analyse des Ausgangsdokuments durch die Analyseeinheit wie folgt aussehen:

Satz 1 (1, 2, 3, 4) Satz 2 (1, 2, 3),

während die Informationskomponentenspeichereinheit 60 dieser strukturellen Analyse entsprechenden Informationskomponenten, also Worte enthält:

(1.1) Peter
(1.2) geht
(1.3) um 20.00 Uhr
(1.4) zum Bahnhof
(2.1) der Zug
(2.2) ist
(2.3) pünktlich

Mit dieser für das nachfolgende Vornehmen der Verschlüsselungsoperationen wichtigen Vorbereitung ist es nunmehr möglich, sowohl auf die einzelnen Informationskomponenten (im

vorliegenden Beispiel die einzelnen Worte), als auch auf die Folgen von Informationskomponenten bzw. Strukturen die Basisoperationen der semantischen Verschlüsselung durchzuführen, nämlich das Vertauschen, Entfernen, Hinzufügen oder Austauschen. Dabei liegt eine wesentliche Schutzwirkung der erfindungsgemäßen semantischen Verschlüsselung darin, dass diese Operationen nicht beliebig durchgeführt werden, sondern dass dies vielmehr unter Beibehaltung der grammatikalischen, syntaktischen und/oder formatmäßigen Regeln erfolgt, so dass auch als Ergebnis der Verschlüsselung ein Resultat entsteht, welches scheinbar (d.h. ohne inhaltliche Prüfung) korrekt zu sein scheint, mit anderen Worten, dem man nicht ansieht, dass es sich in der Tat um ein verschlüsseltes Ergebnis handelt.

Im vorliegenden Ausführungsbeispiel wird mit Hilfe der Verschlüsselungseinheit aus dem oben angegebenen elektronischen Dokument der folgende Text:

Thomas kommt um 16.00 Uhr vom Friedhof. Der Zug ist pünktlich.

Ohne Kenntnis des wahren Inhaltes erscheint dieser Satz also wie ein offenes, unverschlüsseltes Ergebnis, so dass eine wesentliche, schutzbegründende Wirkung der vorliegenden Erfindung bereits darin liegt, dass ein Angreifer angesichts dieses Textes möglicherweise gar nicht erst den Eindruck gewinnt, es handle sich um eine Verschlüsselung, und so von Anfang an einen Angriff auf diesen Text unterläßt.

Konkret wurde im vorliegenden Ausführungsbeispiel durch Wirkung einer Äquivalenzeinheit 70 (die in ihrer einfachsten Fassung als Tabelle bzw. Datenbank von äquivalenten, d.h. entsprechenden und austauschbaren, Begriffen verstanden werden kann, folgendes vorgenommen: Die Inhaltskomponente "Peter" des Ausgangsdokuments wurde durch die grammatikalisch äquivalente Inhaltskomponente "Thomas" ersetzt, wobei Satzstruktur und Grammatik beibehalten wurden, der Sinn des Ursprungsdokuments jedoch bereits zerstört ist. Entsprechend wurde die Inhaltskomponenten "geht" des Ursprungsdokuments in die äquivalente Komponente "kommt" ersetzt, die Inhaltskomponente "um 20.00 Uhr" wurde ersetzt durch "um 16.00 Uhr" (hier wurde durch Wirkung der Äquivalenzeinheit festgestellt, dass es sich um ein numerisches Datum in Form einer Uhrzeit handelt, so dass eine Manipulation innerhalb der zulässigen Uhrzeiten möglich war), und die Inhaltskomponente "zum Bahnhof" wurde ersetzt durch die Inhaltskomponente "vom Friedhof". Dabei wurde zudem durch eine ebenfalls mit der Verschlüsselungseinheit 64 verbundene, den geschilderten Verschlüsselungsbetrieb beeinflussende semantische Regeleinheit 72 sichergestellt, dass das Verschlüsselungsergebnis "...kommt ... vom Friedhof" grammatikalisch und syntaktisch korrekt ist, insoweit also nicht als manipuliert identifiziert werden kann. (Auch das zusätzliche "zum" wäre hier korrekt). Auch wurde mittels der Verschlüsselungseinheit 64 und der zusammenwirkenden Äquivalenzeinheit

70 bzw. semantischen Regeleinheit 72 festgestellt, dass die Inhaltskomponente "der Zug" des nachfolgenden Satzes in einem inhaltlichen Bezug zu der in den vorhergehenden Satz neu eingebrachten Inhaltskomponente "Friedhof" steht, so dass selbst ohne eine Verschlüsselung des zweiten Satzes ein völlig anderer Sinn (und damit ein Verschlüsselungseffekt) entsteht.

Als Ergebnis dieser beschriebenen, einfachen Verschlüsselungsoperationen wird somit das Verschlüsselungsergebnis

"Thomas kommt um 16.00 Uhr vom Friedhof. Der Zug ist pünktlich."

als Volumendaten ausgegeben und in einer Volumendaten-Speichereinheit abgelegt, während ein das Rekonstruieren ermöglichender Schlüssel (im vorliegenden Ausführungsbeispiel eine Information über die jeweils vertauschten Worte mit deren Position im Satz sowie in jeweiligen inhaltlichen Begriffen) in einer Schlüsseldaten-Speichereinheit 74 abgelegt wird. Entsprechend könnte die zugehörige Schlüsseldatei für die Speichereinheit 74 wie folgt aussehen (im folgenden Beispiel wird von der Rekonstruktionseinheit der Befehl EXCHANGE interpretiert, um die im Argument angegebene Vertauschung durchzuführen):

EXCHANGE (1.1; Thomas)
EXCHANGE (1.2; kommt)

usw.

In einer Weiterbildung dieser Ausführungsform ist das Vokabular der Befehlssprache selbst dynamisch und kann durch Funktionen einer Scriptsprache geändert werden; der Befehl EXCHANGE würde so selbst durch einen anderen, beliebigen Ausdruck ersetzt werden können.

Gemäß einer weiteren bevorzugten Ausführungsform der Erfindung ist vorgesehen, eine Mehrzahl von Schlüsseldateien zu erzeugen, von denen jedoch nur eine das korrekte Rekonstruktionsergebnis erzeugt. Schlüsseldatei 2 könnte entsprechend wie folgt beginnen:

EXCHANGE (1.1; Rüdiger)
(Rest wie obige Schlüsseldatei);

Schlüsseldatei beginnt mit:

EXCHANGE (1.1; Claus)

usw.

Im Ausführungsbeispiel der Fig. 2 ist zusätzlich diesen beiden Speichereinheiten eine Ausgabeeinheit 78 nachgeschaltet, die in besonders einfacher Weise die Schlüsseldaten 74 in Form eines Scripts aufbereitet und als lauffähige Scriptdatei 84 ausgeben kann; dies geschieht mit Hilfe einer Konvertierungseinheit 80, welche in ansonsten bekannter Weise aus den Volumendaten der Speichereinheit 76 ein der verschlüsselten Fassung entsprechendes Volumendokument 82 erzeugt, und aus den Index- bzw. Rekonstruktionsdaten der Speichereinheit 74 ein selbständig im Rahmen einer geeigneten Ablaufumgebung lauffähige(s) Strukturbeschreibung, Script, z.B. als Javascript, XML, VB-Script od.dgl., und welches dann selbständig beim Ablaufen das Volumendokument 82 bearbeitet und in die ursprüngliche, unverschlüsselte Form zurückführen kann.

Das als Weiterbildung der vorliegenden Erfindung beschriebene Vieraugenprinzip -- zusätzlich können zwei Dritte das verschlüsselte Dokument durch aufeinanderfolgendes Anwenden ihres jeweiligen Einzelschlüssels entschlüsseln -- kann dadurch implementiert werden, dass, am vorbeschriebenen Beispiel, ein Dritter alle Namen und alle Zeiten/Zahlen entschlüsseln kann, der zweite die sonstigen Inhaltsbestandteile des Dokuments (einschließlich der Reihenfolgen).

Insbesondere im Rahmen einer Internet-Umgebung, wo dann das Volumendokument schon lokal vorhanden oder auf anderem Wege zu einem Nutzer herangeführt worden ist, kann dann über eine gesicherte (und insbesondere auch zum Durchführen einer geeigneten, einem ordnungsgemäßen Zugriff auf das Dokument autorisierenden Identifikations- und/oder Bezahlungsvorgang) die Scriptdatei 84 zu dem autorisierten Benutzer übertragen werden, und dieser kann dann komfortabel (und idealerweise ohne überhaupt mit dem verschlüsselten Volumendokument konfrontiert zu werden) die offene Originalfassung wieder herstellen.

Zusätzlich ist die in Fig. 2 schematisch gezeigte Ausführungsform geeignet, nicht nur eine Schlüsseldatei für die Speichereinheit 74 (bzw. als lauffähige Scriptdatei 84) zu erzeugen, sondern eine Mehrzahl, von denen idealerweise jedoch wiederum nur eine zu einem inhaltlich

tatsächlich korrekten Ergebnis führt, während andere Schlüsseldateien als Scripte einen Entschlüsselungsvorgang auslösen, welcher zwar ebenfalls zu einem sinnvollen (und damit scheinbar korrekten) Ergebnis führt, inhaltlich jedoch nicht mit der Ursprungsfassung übereinstimmt. Hierdurch ist dann eine weitere Erhöhung der Verschlüsselungssicherheit gegeben. Dabei sollte es unmittelbar einsichtig sein, dass bereits geringe inhaltliche Abweichungen den (für einen Nutzer eigentlich wertbildenden) Sinn des Ursprungsdokuments vollständig zerstören, so dass es möglicherweise nur geringer Modifikationen bzw. einer geringen Anzahl von Verschlüsselungsoperationen (mit der Folge einer entsprechend kurzen Scriptdatei als Schlüsseldaten) bedarf, um den vorgesehenen Schutzzweck zu erreichen, bis hin zur bereits erwähnten Nicht-Verschlüsselung der Ursprungsdatei, die ihren Schutzzweck lediglich aus dem Umstand herleitet, dass ein unberechtigt Zugreifender die Unsicherheit hat, ob er es mit einem offenen (d.h. der Ursprungsdatei auch entsprechenden) Inhalt, oder aber mit einem verschlüsselten, d.h. nicht mit der Ursprungsdatei übereinstimmenden Inhalt zu tun hat.

Die vorliegende Erfindung ist nicht auf das exemplarische Beispiel von Textdateien beschränkt. So bietet es sich insbesondere auch an, jegliche weiteren elektronischen Dokumente durch die prinzipiell beschriebene Weise zu verschlüsseln, solange diese elektronischen Dokumente eine für die Basisoperationen des Vertauschens, Entfernens, Hinzufügens oder Austauschens geeignete Struktur aus Inhaltskomponenten aufweisen. Typische weitere Anwendungsfälle wären also insbesondere Musikdatein, die üblicherweise im sog. MP3-Format vorliegen, und wo es im Rahmen der vorliegenden Erfindung möglich ist, die durch das MP3-Format vorgegebenen Datenstrukturen (sog. Frames) einzeln oder blockweise (idealerweise auch takt- oder abschnittsweise, bezogen auf das jeweilige Musikstück) auszutauschen, zu entfernen oder zu vertauschen. Entsprechendes gilt für Bild- und/oder Videodateien, denn auch die dort gängigen, bekannten Dokumentformate basieren auf einer Folge von Frames als Inhaltskomponenten (bei Bildern oder elektronischen Videos sind dies die jeweiligen Einzelbilder), die in der erfindungsgemäßen Weise manipuliert werden können. So ist es hier insbesondere Aufgabe der (auf technische Standards bezogenen) semantischen Regeleinheit (Fig. 2), innerhalb derartiger komplexer Datenstrukturen Ansatzpunkte für eine wirksame Manipulation aufzufinden. Entsprechendes gilt für Farb-, Kontrast-, Helligkeits- oder andere Werte, die im Rahmen einer Darstellungs- oder Ablauflogik des betreffenden Dokuments benutzt werden und mit den Basisoperationen der semantischen Verschlüsselung geändert werden können.

PATENTANSPRÜCHE

1. Datenverarbeitungsvorrichtung mit

- einem einer lokalen Rechnereinheit (10) zugeordneten lokalen Dateiablagesystem (12) zum Abrufen und zur Speicherung sowie zur bidirektionalen Datenübertragung von Volumendateien mittels der Rechnereinheit (10)
- und einer der lokalen Rechnereinheit zugeordneten Nutzer-Identifikationseinheit (20), die zum Ermöglichen eines Zugriffs durch die Rechnereinheit auf für einen Nutzer autorisierte Volumendateien nur als Reaktion auf dessen positive Identifikation ausgebildet ist,
- wobei die Volumendatei in dem lokalen Dateiablagesystem (12) in einer für einen Nutzer nicht brauchbaren, verschlüsselten Form gespeichert ist,

gekennzeichnet durch

- eine einem Datenübertragungspfad von Volumendateien zwischen der lokalen Rechnereinheit (10) und dem lokalen Dateiablagesystem (12) zugeordnete Schlüsselverwaltungseinheit (16) als Teil und Funktionalität der lokalen Rechnereinheit (10), die zum Erzeugen und Zuweisen mindestens einer nutzerspezifischen und volumendateispezifischen Schlüsseldatei für jede Volumendatei ausgebildet ist,
- die Schlüsselverwaltungseinheit (16) mit einer als Teil des lokalen Dateiablagesystems, von diesem logisch getrennt vorgesehenen Schlüsseldatenbank (18) verbunden ist
- und zum Verknüpfen einer in der Schlüsseldatenbank (18) gespeicherten Schlüsseldatei mit einer im lokalen Dateiablagesystem (12) gespeicherten Volumendatei zum Erzeugen eines für einen Nutzer brauchbaren elektronischen Dokuments
- wobei die Schlüsseldatenbank lokal in der Datenverarbeitungsvorrichtung, jedoch logisch oder strukturell oder physisch getrennt von einer dem lokalen Dateiablagesystem zugeordneten Laufwerks- oder Massenspeichereinheit vorgesehen ist.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass die verschlüsselte Form das Verschlüsseln mittels eines symmetrischen Schlüssels aufweist.

3. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass die verschlüsselte Form ein bezogen auf ein elektronisches Dokument als Basis für eine Volumendatei inhalts- und/oder sinnentstellendes Vertauschen, Entfernen und/oder Hinzufügen von Dateikomponenten aufweist.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das lokale Dateiablagesystem (12) eine Datenbank und die Volumendateien Datenbankeinträge oder Datensätze der Datenbank sind.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das lokale Dateiablagesystem (12) eine Arbeitsplatz-Massenspeichereinheit für bevorzugt eine Mehrzahl von Nutzern ist.

6. Vorrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Volumendateien digitale Text-, Programm-, Bild-, Audio- und Videodateien sowie Kombinationen aus diesen aufweisen.

7. Verfahren zur Speicherung und zum Aufruf von elektronischen Dateien, insbesondere zum Betreiben einer Datenverarbeitungsvorrichtung nach einem der Ansprüche 1 bis 6, gekennzeichnet durch die Schritte:

- Identifizieren eines an einer Rechnereinheit zum Zugreifen auf in einem der Rechnereinheit zugeordneten Dateiablagesystem gespeicherten oder zu speichernden Volumendateien tätigen Nutzers;
- Ermöglichen des autorisierten Zugriffs auf nutzerspeizifische Volumendateien als Reaktion auf eine positive Identifikation;
- Erzeugen einer volumendatei- und nutzerspezifischen Schlüsseldatei für ein im Dateiablagesystem zu speicherndes elektronisches Dokument und nachfolgendes Verknüpfen des elektronischen Dokuments mit der Schlüsseldatei zum Erzeugen und Speichern einer für einen Nutzer nicht brauchbaren Volumendatei;
- Ablegen der erzeugten Schlüsseldatei in einer Schlüsselspeichereinheit;
- Auslesen einer volumendatei- und nutzerspezifischen Schlüsseldatei als Reaktion auf einen Zugriffsbefehl eines Nutzers;
- Verknüpfen der ausgelesenen Schlüsseldatei mit einer aus dem Dateiablagesystem ausgelesenen, für einen Nutzer nicht brauchbaren Volumendatei zum Erzeugen eines brauchbaren elektronischen Dokuments.

8. Verfahren zum Verschlüsseln einer elektronisch gespeicherten ursprünglichen Datenmenge, insbesondere als Verfahren zum Erzeugen einer volumendatei- und nutzerspezifischen Schlüsseldatei nach Anspruch 7 und/oder zum Betreiben der Schlüsselverwaltungseinheit in der Vorrichtung nach einem der Ansprüche 1 bis 6, wobei die elektronisch gespeicherte ursprüngliche Datenmenge aus einer Folge von Informationskomponenten einer Metasprache in Form einer Schriftsprache, eines Zahlensystems oder von Informationskomponenten aus in einer vorbestimmten, einheitlichen Formatstruktur angeordneten Datenelementen, insbesondere Bild-, Ton- oder Programminformationen, besteht und in einer Mehrzahl von elektronisch adressierbaren Speicherbereichen gespeichert ist, mit den Schritten:

- Vertauschen und/oder Entfernen einer Informationskomponente in der Datenmenge und/oder Hinzufügen einer Informationskomponente an eine vorbestimmte Position in der Folge von Informationskomponenten und/oder Austauschen einer Informationskomponente gegen eine bevorzugt in der ursprünglichen Datenmenge nicht enthaltene Informationskomponente durch einen Rechnerzugriff auf einen jeweiligen der Speicherbereiche zum Erzeugen einer verschlüsselten Datenmenge;
- Erzeugen einer Schlüsseldatenmenge mit Angaben über die vertauschten, entfernten, hinzugefügten und/oder ausgetauschten Informationskomponenten, die so ausgebildet ist, dass sie ein Wiederherstellen der ursprünglichen Datenmenge gestattet und
- Abspeichern der verschlüsselten Datenmenge sowie Abspeichern der Schlüsseldatenmenge in einer getrennten, benutzerindividualisierten Schlüsseldatei eines gemeinsamen Dateisystems.

9. Verfahren nach Anspruch 8, gekennzeichnet durch das aufeinanderfolgende, mindestens zweifache Verschlüsseln der Schlüsseldatenmenge jeweils durch den Schritt des Vertauschens, Entfernens, Hinzufügens und/oder Austauschens, wobei ein erster, hierdurch erzeugter Schlüsseldatensatz einem ersten Benutzer und ein zweiter, nachfolgend erzeugter Schlüsseldatensatz einem zweiten Benutzer zugeordnet wird.

10. Vorrichtung zum Behandeln einer elektronisch gespeicherten ursprünglichen Datenmenge, insbesondere zur Durchführung des Verfahrens nach einem der Ansprüche 7 oder 8 und/oder als Bestandteil der Schlüsselverwaltungseinheit in der Vorrichtung nach einem der Ansprüche 1 bis 6 mit

- einer Analyseeinheit (54, 56), die zum Zugreifen auf die in einer Dokumentspeichereinheit (52) gespeicherte ursprüngliche Datenmenge sowie zum elektronischen Erfassen von mindestens einer Folge von Informationskomponenten der ursprüngli-

chen Datenmenge als Reaktion auf vorbestimmte und/oder ermittelte Format- und/oder Strukturdaten der ursprünglichen Datenmenge ausgebildet ist,

- einer der Analyseeinheit nachgeschalteten Verschlüsselungseinheit (64), die zum

  Vertauschen und/oder Entfernen einer Informationskomponente in der ursprünglichen Datenmenge und/oder Hinzufügen einer Informationskomponente an eine vorbestimmte Position in der Folge von Informationskomponenten und/oder Austauschen einer Informationskomponente gegen eine bevorzugt in der ursprünglichen Datenmenge nicht enthaltene Informationskomponente sowie zum

  Erzeugen einer Schlüsseldatenmenge mit Angaben über die vertauschten, entfernten, hinzugefügten und/oder ausgetauschten Informationskomponenten, die so gebildet ist, dass sie ein Wiederherstellen der ursprünglichen Datenmenge gestattet,

ausgebildet ist,

- einer zum Abspeichern der Schlüsseldatenmenge ausgebildeten Schlüsseldatenspeichereinheit (74) sowie
- einer zum Abspeichern der verschlüsselten Datenmenge ausgebildeten Volumendatenspeichereinheit (76).

11. Vorrichtung nach Anspruch 10, dadurch gekennzeichnet, dass der Verschlüsselungseinheit (64) eine Äquivalenzeinheit (70) zugeordnet ist, die für mindestens eine Informationskomponente in der ursprünglichen Datenmenge mindestens eine Äquivalenzinformationskomponente elektronisch gespeichert bereithält, wobei die Äquivalenzinformationskomponente so gebildet ist, dass sie mit der zugehörigen Informationskomponente grammatikalisch, formatmäßig, metaphorisch und/oder syntaktisch übereinstimmt.

12. Vorrichtung nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass die Verschlüsselungseinheit zum Zusammenwirken mit einer semantischen Regeleinheit (72) ausgebildet ist, die so eingerichtet ist, dass das Vertauschen, Entfernen, Hinzufügen oder Austauschen innerhalb der/des Grammatik, Formats, Metaphorik und/oder Syntax erfolgt, die/das durch die Format- und/oder Strukturdaten bestimmt ist.

13. Vorrichtung nach einem der Ansprüche 10 bis 12, dadurch gekennzeichnet, dass der Verschlüsselungseinheit eine Zufallssteuerungseinheit (68) zugeordnet ist, die das Vertauschen, Entfernen, Hinzufügen und/oder Austauschen durch die Verschlüsselungseinheit betreffend einzelne Informationskomponenten und/oder Folge(n) von Informationskomponenten zufallsabhängig, insbesondere nicht reproduzierbar, steuert.

14. Vorrichtung nach einem der Ansprüche 10 bis 13, gekennzeichnet durch eine der Verschlüsselungseinheit zugeordnete Verschlüsselungsparametereinheit (66), die zum Speichern und/oder Einstellen vorbestimmter Parameter für das Vertauschen, Entfernen, Hinzufügen und/oder Austauschen durch die Verschlüsselungseinheit ausgebildet ist, insbesondere betreffend eine durch eine Anzahl des Vertauschens, Entfernens, Hinzufügens und/oder Austauschens erreichte Verschlüsselungstiefe.

15. Vorrichtung nach einem der Ansprüche 10 bis 14, gekennzeichnet durch eine der Verschlüsselungseinheit nachgeschaltete Konvertierungseinheit (80), die zum Erzeugen einer elektronisch übertragbaren Volumendatei aus der verschlüsselten Datenmenge sowie einer bevorzugt aktiv ablauffähigen Programm- und/oder Scriptdatei aus der Schlüsseldatenmenge ausgebildet ist.

16. Vorrichtung nach einem der Ansprüche 10 bis 15, dadurch gekennzeichnet, dass die Verschlüsselungseinheit zum Erzeugen einer Mehrzahl von Schlüsseldatenmengen ausgebildet ist, von denen mindestens eine bei einem Zusammenführen mit der verschlüsselten Datenmenge nicht das Wiederherstellen der ursprünglichen Datenmenge gestattet, jedoch nach dem Zusammenführen zu einer Datenmenge führt, die mit der ursprünglichen Datenmenge syntaktisch, formatmäßig und/oder grammatikalisch übereinstimmt.

17. Vorrichtung nach einem der Ansprüche 10 bis 16, dadurch gekennzeichnet, dass die der Analyseeinheit nachgeschaltete Verschlüsselungseinheit in der Schlüsseldatenmenge zum Aus- oder Vertauschen der Angaben über die vertauschten, entfernten, hinzugefügten und/oder ausgetauschten Informationskomponenten ausgebildet ist.

Fig. 1

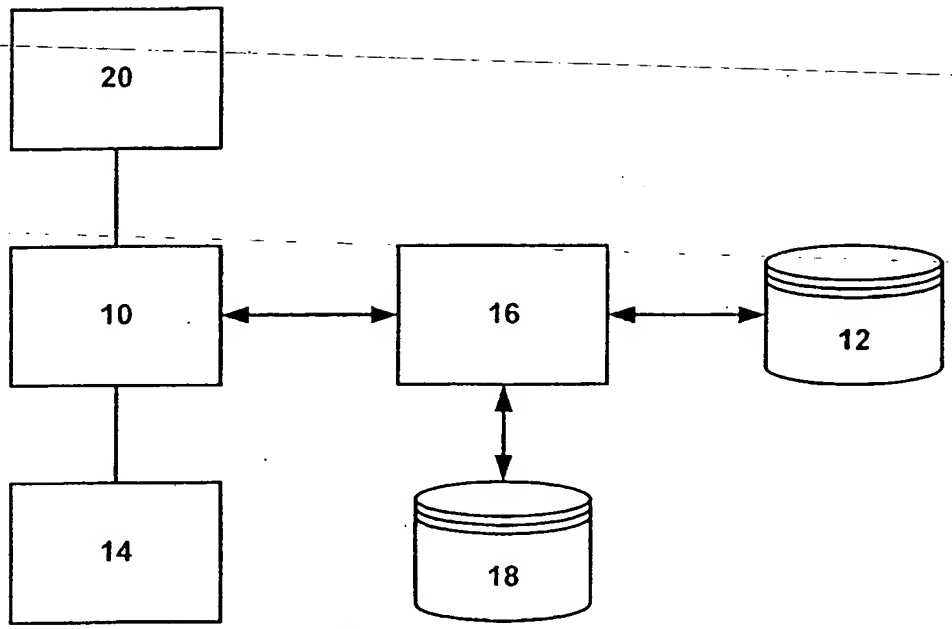
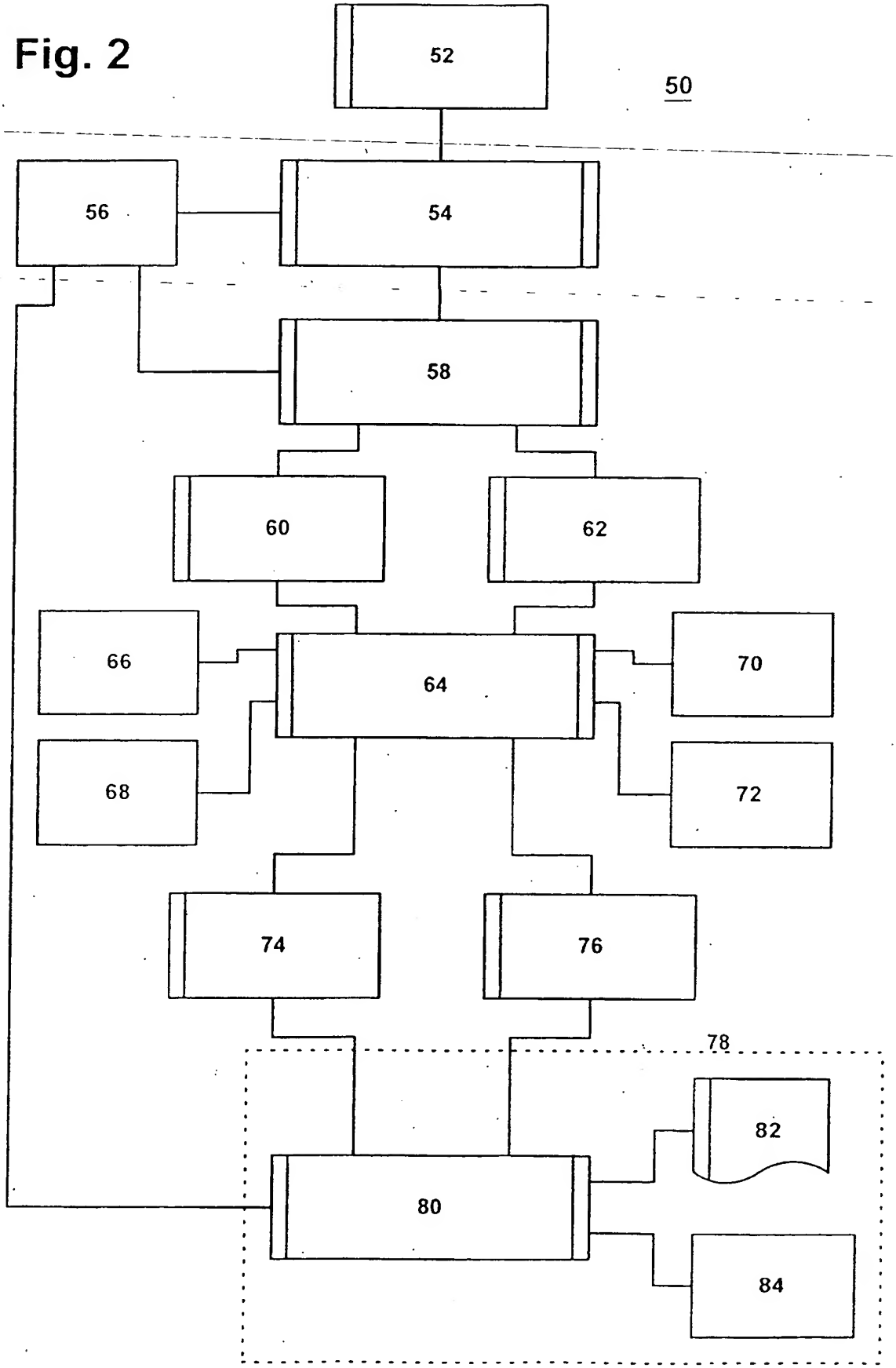


Fig. 2



INTERNATIONAL SEARCH REPORT

Internati , Application No
PCT/EP 00/06824

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 765 152 A (ERICKSON JOHN S) 9 June 1998 (1998-06-09) figures 1,2,4-6,9 column 2, line 61 -column 4, line 15 column 7, line 12 -column 8, line 57	1-3,5-8, 10,15
A	EP 0 567 800 A (IBM) 3 November 1993 (1993-11-03) figures 1-3 column 8, line 30 -column 11, line 19	1,4,6,7

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 December 2000	14/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internati . Application No
PCT/EP 00/06824

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5765152 A	09-06-1998	AU 7662496 A	30-04-1997
		WO 9714087 A	17-04-1997
EP 0567800 A	03-11-1993	JP 2659896 B	30-09-1997
		JP 6103286 A	15-04-1994
		US 5532920 A	02-07-1996

INTERNATIONALER RECHERCHENBERICHT

Internati es Aktenzeichen
PCT/EP 00/06824

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 765 152 A (ERICKSON JOHN S) 9. Juni 1998 (1998-06-09) Abbildungen 1,2,4-6,9 Spalte 2, Zeile 61 -Spalte 4, Zeile 15 Spalte 7, Zeile 12 -Spalte 8, Zeile 57	1-3,5-8, 10,15
A	EP 0 567 800 A (IBM) 3. November 1993 (1993-11-03) Abbildungen 1-3 Spalte 8, Zeile 30 -Spalte 11, Zeile 19	1,4,6,7

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
7. Dezember 2000	14/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internat. ...s Aktenzeichen
PCT/EP 00/06824

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5765152 A	09-06-1998	AU 7662496 A	30-04-1997
		WO 9714087 A	17-04-1997
EP 0567800 A	03-11-1993	JP 2659896 B	30-09-1997
		JP 6103286 A	15-04-1994
		US 5532920 A	02-07-1996